THE FARFALLE MYSTERY

SERGE CANTAT, FRANÇOIS MAUCOURANT, AND YAGO MORENO

ABSTRACT. In 2017, for the π-day, Mickaël Launay described a remarkable property of the Fibonacci sequence, which he called "le mystère de la farfalle". The name farfalle refers to a shape of pasta that is famous in France, pastas that Mickaël Launay cooked on stage during his general public lecture. He proposed a prize of 3.14 Euros to whom will explain the phenomenon he had discovered. We provide such an explanation, which illustrates recent works by Kurlberg and Rudnick, and by Bourgain and Glibichuk.

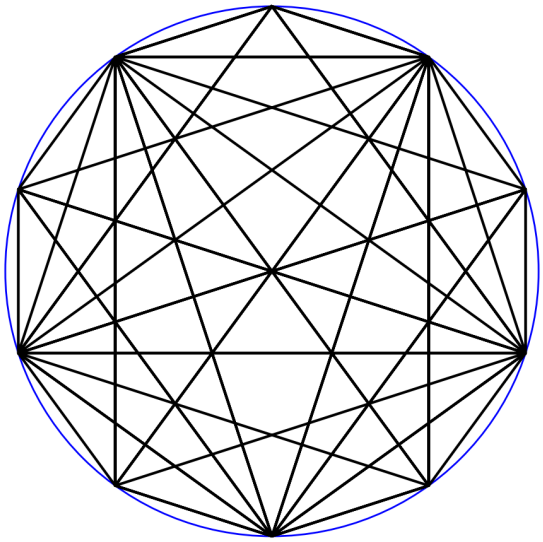

FIGURE 1. The Fibonacci sequence modulo 10, in Launay's representation.

Date: 2022.

1. Le mystère de la Farfalle, according to Mickaël Launay

The **Fibonacci sequence** (F_n) is the bi-infinite sequence defined by the initial values $F_0 = 0$, $F_1 = 1$ and the linear recursion $F_n = F_{n-1} + F_{n-2}$. It can also be calculated via the recursion

$$\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.1}$$

where

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}. \tag{1.2}$$

We shall call A the **Fibonacci matrix**. Its determinant is -1 and its eigenvalues are the golden mean and its Galois conjugate:

$$\varphi = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \varphi' = \frac{1-\sqrt{5}}{2} = -\frac{1}{\varphi}. \tag{1.3}$$

If N is a positive integer, then $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is a finite group, the **order** $\mathrm{ord}_A(N)$ of A in this group is finite, and the Fibonacci sequence is periodic modulo N. Its period and $\mathrm{ord}_A(N)$ are equal, and called the **Pisano period**. We refer to Sections 3.3 and 4 below for the study of $\mathrm{ord}_A(\cdot)$.

Denote by $\mathbb{S}^1$ the unit circle:

$$\mathbb{S}^1 = \{z \in \mathbf{C}\ ;\ |z| = 1\} = \{e^{2i\pi\theta}\ ;\ \theta \in \mathbf{R}/\mathbf{Z}\}; \tag{1.4}$$

it is a multiplicative subgroup of $\mathbf{C}^*$. The map

$$a \in \mathbf{Z}/N\mathbf{Z} \ \mapsto\ e^{2i\pi a/N} \in \mathbb{S}^1 \tag{1.5}$$

provides an isomorphism from the additive group $\mathbf{Z}/N\mathbf{Z}$ to the multiplicative group of roots of unity of order dividing N. Two points z and z' of $\mathbb{S}^1$ determine a chord, namely the segment $[z, z'] \subset \mathbf{C}$ joining them. Thus, a finite sequence $(z_i)_{i=0}^{\ell}$ determines a finite set of chords $[z_0, z_1]$, …, $[z_{\ell-1}, z_\ell]$ that form a continuous piecewise linear curve in the closed unit disk. Similarly, a periodic sequence $(z_i)_{i\in\mathbf{Z}}$, of period q, determines a finite set of (at most) q successive chords $[z_i, z_{i+1}]$. Mickaël Launay applied this construction to the sequence

$$z_i = \exp(2i\pi F_i/N), \tag{1.6}$$

which depends only on F_i modulo N. Figures 1 and 2 provide a sample of images. As one can see, for some specific values of N the chords cluster to a farfalle (or butterfly) shape made of four chords. Our first result will, indeed, show that the farfalle's shape occurs when N is of type $5F_k$ for some $k \geq 2$.

Then, we shall explain why such a specific shape does not occur for random, or general values of N.

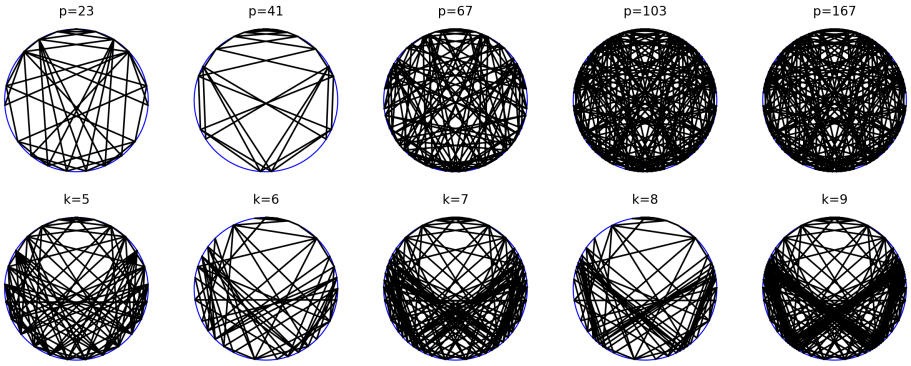

FIGURE 2. Ten examples of Launay's chord representation of the Fibonacci sequence modulo N. On the top, N is a prime. On the bottom, N is equal to $5F_k$ for $k = 5, 6, 7, 8, 9$; the Farfalle shows up progressively. Each figure on top corresponds to the nearest prime approximation to $5F_k$ for the figure below it.

2. THE FARFALLE MYSTERY AND ANOSOV DYNAMICS ON THE TORUS

This section describes another viewpoint on Launay's question, and states our main results.

2.1. **The space of chords.** To a pair of points $(z, z') \in \mathbb{S}^1 \times \mathbb{S}^1$ corresponds a unique (oriented) chord $[z, z']$, and vice versa; the diagonal corresponds to chords $[z, z]$ of length 0. Thus, the space of chords is a 2-dimensional torus

$$\mathbb{S}^1 \times \mathbb{S}^1 \simeq \mathbf{R}/\mathbf{Z} \times \mathbf{R}/\mathbf{Z} = \mathbf{R}^2/L \tag{2.1}$$

where $L \subset \mathbf{R}^2$ is the square lattice $\mathbf{Z}^2$. Let O denote the image of $(0, 0)$ in $\mathbf{R}^2/L$. Then, $\mathbf{R}^2/L$ is a 2-dimensional, additive Lie group with neutral element O. The natural projection

$$\pi \colon \mathbf{R}^2 \to \mathbf{R}^2/L \tag{2.2}$$

is a group homomorphism, with kernel L, and is the universal cover of $\mathbf{R}^2/L$.

2.2. **Linear transformations of the torus.** Let B be a 2-by-2 matrix with integer coefficients. It acts linearly on $\mathbf{R}^2$, preserving the lattice L, and induces a smooth homomorphism $f_B\colon \mathbf{R}^2/L \to \mathbf{R}^2/L$. When B has determinant 1 or -1 its inverse has integer coefficients too and f_B is an isomorphism, the inverse of which is $f_{B^{-1}}$. We shall say that f_B is the **linear transformation** (or linear diffeomorphism if $\det(B) = \pm 1$) induced by B. In this way, we obtain a homomorphism $B \mapsto f_B$ from $\mathsf{GL}_2(\mathbf{Z})$ to the group of linear diffeomorphisms of $\mathbf{R}^2/L$. When $B \in \mathsf{GL}_2(\mathbf{Z})$ has two eigenvalues such that $|\lambda| > 1 > |\lambda'|$, then f_B is an **Anosov**, linear diffeomorphism. For instance, the Fibonacci matrix A induces such a linear Anosov diffeomorphism

$$f_A\colon \mathbf{R}^2/L \to \mathbf{R}^2/L. \tag{2.3}$$

2.3. **Small orbits.** If N is a positive integer, the map $\iota_N\colon \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z} \to \mathbf{R}^2/L$ defined by $\iota_N(a,b) = (a/N, b/N)$ is a homomorphism of additive groups. It conjugates

- the action of f_A on the finite set $\frac{1}{N}\mathbf{Z}^2/L \subset \mathbf{R}^2/L$
- the action of A, via its reduction in $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$, on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$.

We shall identify these two actions without further notice. The f_A-orbit of $(a/N, b/N)$ is finite and its period divides $\mathrm{ord}_A(N)$. Conversely, if $P \in \mathbf{R}^2/L$ is f_A-periodic, of period q, then $A^q(P) = P + V$ for some $V \in L$. From this, one easily gets: *A point $P \in \mathbf{R}^2/L$ is f_A-periodic if and only if $P \in \mathbf{Q}^2/L$, if and only if P is in the image of ι_N for some N.*

Coming back to Launay's modular representation of the Fibonacci sequence, the chord $[e^{2i\pi F_n/N}, e^{2i\pi F_{n+1}/N}]$ corresponds to the point $(F_n/N, F_{n+1}/N) \in \mathbf{R}^2/L$. Since $A(F_n/N, F_{n+1}/N) = (F_{n+1}/N, F_{n+2}/N)$, *the finite sequence of chords drawn by Launay corresponds exactly to the finite orbit of*

$$P_N := (F_0/N, F_1/N) = (0/N, 1/N) \tag{2.4}$$

under the action of f_A on $\mathbf{R}^2/L$.

Proposition 2.1 (Periodic orbits of small order)**.** *The linear diffeomorphism $f_A\colon \mathbf{R}^2/L \to \mathbf{R}^2/L$ has exactly one fixed point, namely the origin $O = (0,0)$* mod (L)*, no periodic orbit of period* 2*, and*

- *a unique orbit of period* 3*, namely* $\{(0,1/2), (1/2,1/2), (1/2,0)\}$*;*
- *a unique orbit of period* 4*,*

$$\{(2/5,1/5), (1/5,3/5), (3/5,4/5), (4/5,2/5)\};$$

- *two orbits of period* 5*, namely* $\{(3k/11,k/11)\ ;\ k=1,4,5,9,3\}$*, and* $\{(3k/11,k/11)\ ;\ k=2,8,10,7,6\}$.

The proof is straightforward. Figure 3 shows the orbit of period 4; it suggests that *the shape of the farfalle is given by the orbit of period* 4.

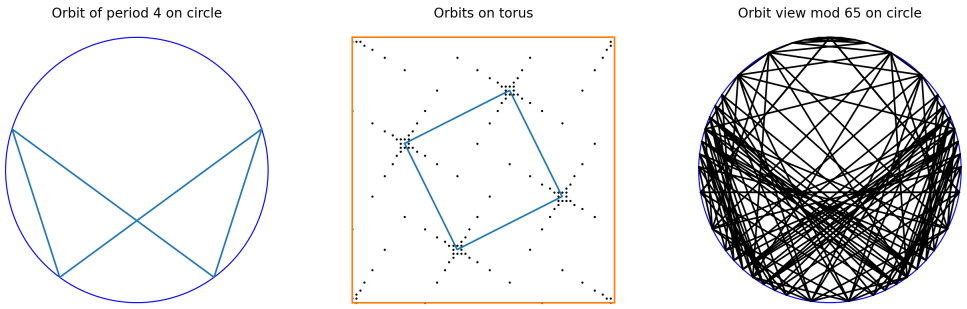

FIGURE 3. In the middle, one sees the orbit of P_N for $N = 65 = 5F_7$ drawn on the torus, as well as a square showing the orbit $\{(2/5,1/5),(1/5,3/5),(3/5,4/5),(4/5,2/5)\}$. On the left, one sees Launay's representation of this orbit of period 4. And on the right, Launay's representation of the Fibonacci sequence modulo 65.

Comparing this picture with Launay's approximate farfalles (Figure 2), one may ask: For which values of N does the f_A-orbit of P_N in $\mathbf{R}^2/L$ spend a large part of its time near the orbit of period 4 of f_A? This is not the right question. Indeed, since P_N is close to the origin O when N is large and f_A is continuous, the orbit $f_A^n(P_N)$ stays close to O when n is small; these points correspond to the short chords $[e^{2i\pi F_n/N}, e^{2i\pi F_{n+1}/N}]$, with $F_n \ll N$ ([1]). Adding the origin to the orbit of period 4, one gets a set G of 5 elements:

$$G = \{O,(2/5,1/5),(1/5,3/5),(3/5,4/5),(4/5,2/5)\} \subset \mathbf{R}^2/L; \qquad (2.5)$$

as we shall see in Section 3.1, G is a subgroup of $\mathbf{R}^2/L$. Now, the question raised by Mickaël Launay becomes:

Question 2.1 (Launay's question on $\mathbf{R}^2/L$)**.** For which values of N does the f_A-orbit of the point P_N in $\mathbf{R}^2/L$ spend a large part of its time near G?

[1]Given two sequences (a_n) and (b_n) of positive numbers, we write $a_n = o(b_n)$ or $a_n \ll b_n$ if a_n becomes negligible with respect to b_n as n goes to $+\infty$; we write $a_n \lesssim b_n$ if $a_n \le Cb_n$ for some constant $C > 0$ and large enough n.

This question includes two distinct problems:

1.– We shall exhibit specific values of N for which most of the points in the orbit of P_N are located near G. Of course, these special values need to match the ones found by Mickaël Launay! This is not hard, but somewhat surprising. See Theorem A below.

2.– For most values of N, we shall show that the orbit of P_N does not cluster near G. Two strategies will be applied. The first one is based on entropy estimates, and holds for a set of integers $N \in \mathbf{N}$ of density 1. See Theorem B below. The second one relies on Fourier analysis, exponential sums, and sum-product estimates. It gives a better result, namely an equidistribution of the orbit of P_N towards the Haar measure on $\mathbf{R}^2/L$, but it is much harder. See Theorems C and D below.

2.4. **Approximate farfalles.** For N in $\mathbf{N}^*$, we denote by μ_N the probability measure given by averaging on the orbit of P_N:

$$\mu_N = \frac{1}{\mathrm{per}_A(P_N)} \sum_{n=1}^{\mathrm{per}_A(P_N)} \delta_{f_A^n(P_N)} \tag{2.6}$$

where $\mathrm{per}_A(P_N)$ is the **period** of P_N.We shall see in Lemma 3.2 that $\mathrm{ord}_A(N) = \mathrm{per}_A(P_N)$ is the Pisano period. If μ is a probability measure on $\mathbf{R}^2/L$ and (N_j) is an increasing sequence of positive integers, recall that μ_{N_j} converges towards μ if, for every continuous function $\xi\colon \mathbf{R}^2/L \to \mathbf{R}$,

$$\int_{\mathbf{R}^2/L} f\, d\mu_{N_j} = \frac{1}{\mathrm{per}_A(P_{N_j})} \sum_{n=1}^{\mathrm{per}_A(P_{N_j})} \xi(f_A^n(P_{N_j})) \longrightarrow \int_{\mathbf{R}^2/L} \xi\, d\mu \tag{2.7}$$

as N_j goes to $+\infty$.

Theorem A. *Set $N(k) = 5F_k$. Let ε be a positive real number. Then,*

1. *the orbit of $P_{N(k)}$ under f_A is periodic of period $10k$ if k is even, and $20k$ if k is odd;*
2. *the proportion of points in this orbit at distance less than ε from G is larger than $1 - \left\lceil 1 - \frac{\log(\varepsilon/\sqrt{2})}{\log(\varphi)} \right\rceil k^{-1}$;*
3. *the probability measures $\mu_{N(k)}$ converge towards the probability measure $\mu_G := \frac{1}{5}\sum_{g\in G} \delta_g$ as k goes to $+\infty$.*

The first values of N for which Launay observed the farfalle are exactly the $5F_k$ for small values of k. Thus, one can say that Theorem A explains the farfalle mystery, both from a topological and from a stochastic viewpoint.

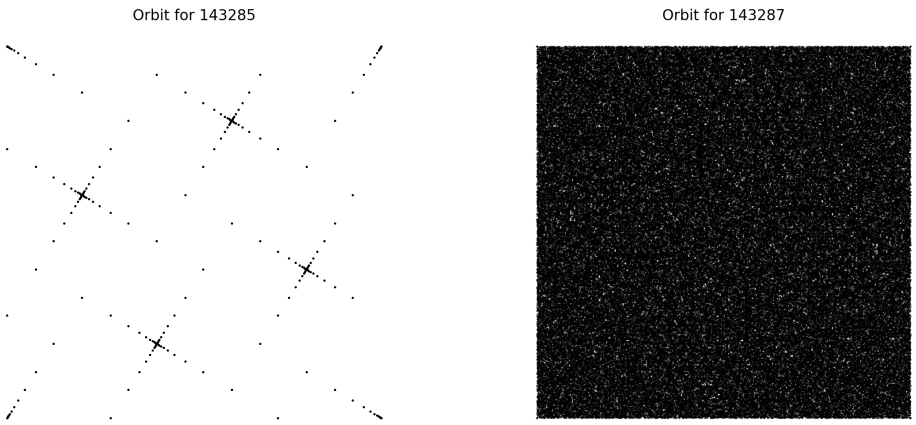

FIGURE 4. On the left, the orbit of P_N on the torus, with $N = 5F_{23} = 143285$. On the right, the orbit of P_N for N equal to the prime number 143287. The first orbit contains only 460 points, while the second contains 286576 points (see Example 4.2).

2.5. **Equidistribution.** On the opposite, we shall show that for most values of N, it is unlikely to witness a farfalle shape in Launay's construction. Recall that a subset K of $\mathbf{N}$ has positive (lower) density if there is a $\delta > 0$ such that

$$\frac{1}{x}|\{N \in K\,;\, N \leq x\}| \geq \delta \tag{2.8}$$

for all large enough values of $x \in \mathbf{R}_+^*$. If the proportion $\frac{1}{x}|\{N \in K\,;\, N \leq x\}|$ converges as x goes to $+\infty$, the limit is called the **density** of K. In particular, K has density 1 if and only if one can take δ arbitrary close to 1 in the Inequality (2.8). By the prime number theorem, the number of primes $p \leq x$ grows like $x/\log(x)$ as x goes to $+\infty$. Thus, for subsets K of the set of prime numbers, the right notion is the **relative density** (among all primes), in which the proportion $\frac{1}{x}|\{N \in K\,;\, N \leq x\}$ is replaced by

$$\frac{1}{x/\log(x)}|\{N \in K\,;\, N \leq x\}. \tag{2.9}$$

The first result we shall prove will be superseded by Theorem C, but its proof is much simpler and illustrates some basic ideas from ergodic theory.

Theorem B. *There is a subset K of $\mathbf{N}$ of density 1 with the following property. If (N_j) is any increasing sequence of integers contained in K and if μ_{N_j}*

converges towards a measure μ, then the Hausdorff dimension of the support of μ is larger than or equal to $1/2$.

In particular, since any finite (or countable) set has dimension 0 (see [4]), the measures μ_N, for N in K, can not cluster to G. Theorem B will be proved in Section 5.4.

Theorem C. *There is a subset K of $\mathbf{N}$ of density 1 with the following property. If (N_j) is any increasing sequence of integers contained in K, then μ_{N_j} converges towards the Haar measure on $\mathbf{R}^2/L$ as j goes to $+\infty$.*

This will be our main result in the direction opposite to Launay's observation. It is obtained in Section 8.3; the proof relies on Fourier analysis, the main computation being described in Section 7. As stated, Theorem C does not say anything of the measures μ_{N_j} when the N_j are prime numbers, but its proof provides also the following result:

Theorem D. *There exists a subset K of the prime numbers, of positive relative density, such that if p_ℓ is any increasing sequence with $p_\ell \in K$, then, μ_{p_ℓ} converges towards the Haar measure on $\mathbf{R}^2/L$ as k goes to $+\infty$.*

In fact, one can say more. It is natural in this setting to distinguish between the primes p such that 5 is a square mod p, or not – i.e. $p \equiv 1$ or $4 \mod (5)$ or $p \equiv 2$ or $3 \mod (5)$ respectively. Among the primes congruent to 2, 3 mod (5), one can take a subset K of full density so that the conclusion of Theorem D holds (Theorem 8.3); this is a direct corollary of a highly non-trivial theorem of Bourgain and Glibichuk [1] and a simple inequality by Erdös and Murty [3].The set of primes congruent to 1, $4 \mod (5)$ also contains a set of positive density such that the analogue of Theorem D holds (Theorem 8.2). Moreover, if one assumes the Generalized Riemann Hypothesis (GRH), a result of Kurlberg [7] shows that the subset K in Theorem D can be chosen of full relative density (Theorem 8.4).

Remark 2.2. The Haar measure is an f_A-invariant probability measure on $\mathbf{R}^2/L$. Fourier analysis shows that a function $\xi \in L^1(\mathbf{R}^2/L, dxdy)$ which is f_A-invariant is almost everywhere constant. By the Birkhoff ergodic theorem, almost every trajectory converges towards the Haar measure; this means that for every continuous function ξ and almost every starting point Q

$$\frac{1}{m}\sum_{n=0}^{m-1} \xi(f_A^n(Q)) \longrightarrow \int_{\mathbf{R}^2/L} \xi \, dxdy \tag{2.10}$$

as m goes to $+\infty$. When such a convergence holds, one says that the orbit of Q is equidistributed with respect to the Haar measure. Of course, if Q is periodic, for instance $Q = P_N$ for some N, then its orbit is not equidistributed. But still, we shall see in Section 8.1 that, in their vast majority, long periodic orbits provide good approximation to the Haar measure. Launay's question is to determine for which values of N the orbit of P_N clusters on a small set (namely the group G) instead of being well distributed; thus, Launay's question concerns a rare and unusual phenomenon.

3. When the farfalle appears

We explain Launay's observation for the sequence $N(k) = 5F_k$.

3.1. **The orbit of period 4 and the group G.** Consider the set G defined in Equation (2.5). It is the union of the origin O and the orbit of period 4. The map $\iota_G\colon a \in \mathbf{Z}/5\mathbf{Z} \mapsto (2a/5, a/5) \in \mathbf{R}^2/L$ is an injective homomorphism of additive groups and its image coincides with G; so, G is a cyclic subgroup of $\mathbf{R}^2/L$ of order 5. It is invariant under the action of $f_A\colon \mathbf{R}^2/L \to \mathbf{R}^2/L$ and ι_G conjugates f_A to the multiplication by 3: $\iota_G(3a) = f_A(\iota_G(a))$ for all $a \in \mathbf{Z}/5\mathbf{Z}$.

3.2. **The "small" torus $\mathbf{R}^2/L_G$.** The pre-image of G in $\mathbf{R}^2$ under the projection $\pi\colon \mathbf{R}^2 \to \mathbf{R}^2/L$ is the lattice L_G of $\mathbf{R}^2$ generated by $(2/5, 1/5)$ and $(1/5, 3/5)$; it is also generated by $(2/5, 1/5)$ and $(-1/5, 2/5)$. The quotient $\mathbf{R}^2/L_G$ is equal to $(\mathbf{R}^2/L)/G$. We shall denote by $\pi_G\colon \mathbf{R}^2 \to \mathbf{R}^2/L_G$ and $\eta\colon \mathbf{R}^2/L \to \mathbf{R}^2/L_G$ the natural projections; then, $\eta^{-1}(0) = G$.

Since f_A preserves G, A preserves L_G and A induces a linear diffeomorphism $g_A\colon \mathbf{R}^2/L_G \to \mathbf{R}^2/L_G$ such that

$$f_A \circ \pi = \pi \circ A, \quad g_A \circ \pi_G = \pi_G \circ A, \quad \text{and} \quad g_A \circ \eta = \eta \circ f_A. \tag{3.1}$$

To study the orbit of P_N under the action of f_A and how this orbit approches G, one may first study the orbit of $\eta(P_N)$ in $\mathbf{R}^2/L_G$ under the action of g_A and how it approches the origin.

Consider the matrix C that maps the basis $((1,0),(0,1))$ of L to the basis $((2/5,1/5),(1/5,3/5))$ of L_G. We have

$$C = \frac{1}{5}\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \quad C^{-1} = \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix}. \tag{3.2}$$

It induces a linear isomorphism $h_C\colon \mathbf{R}^2/L \to \mathbf{R}^2/L_G$. Since $5C = 2A^2 - A$, C commutes to A. Thus, we get the following lemma.

Lemma 3.1. *The linear isomorphism $C\colon \mathbf{R}^2 \to \mathbf{R}^2$ maps the lattice L to the lattice L_G. It induces a linear diffeomorphism $h_C\colon \mathbf{R}^2/L \to \mathbf{R}^2/L_G$ that conjugates the action of f_A on $\mathbf{R}^2/L$ to the action of g_A on $\mathbf{R}^2/L_G$: $h_C \circ f_A = g_A \circ h_C$.*

Since we are interested in the orbit of $\eta(P_N)$ under g_A, we are indeed interested in the orbit of $C^{-1}(P_N) = (-1/N, 2/N)$ under f_A. Since $A(-1/N, 2/N) = \frac{1}{N}(2,1)$, the orbit of $C^{-1}(P_N)$ is the same (after a shift of time $n \mapsto n+1$) as the orbit of

$$Q_N := (2/N, 1/N) \tag{3.3}$$

under f_A. Note that $A^n(Q_N) = \frac{1}{N}(L_n, L_{n+1})$ where (L_n) is the **Lucas sequence**, defined by $L_0 = 2$, $L_1 = 1$, and the same recursion $L_{n+1} = L_n + L_{n-1}$ as the Fibonacci sequence. To sum up, Launay's initial question leads to:

Question 3.1 (Reduction of Launay's question to $\mathbf{R}^2/L_G$)**.** For which values of N does the f_A-orbit of Q_N spend most of its time near the origin O of $\mathbf{R}^2/L$?

Warning.– We shall view the points P_N and Q_N as points in $\mathbf{R}^2/L$ or in $\mathbf{R}^2$ alternatively, without further distinction. For instance, $A^n(P_N)$ will be a point of $\mathbf{R}^2$, while $f_A^n(P_N)$ will be a point in $\mathbf{R}^2/L$.

3.3. **Periods.** Recall that $\mathrm{ord}_A(N)$ is the order of A in $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$. For $P \in \mathbf{R}^2/L$, we denote by $\mathrm{Orb}_A(P)$ its orbit under the action of f_A, and by $\mathrm{per}_A(P)$ its period, with $\mathrm{per}_A(P) = +\infty$ if P is not periodic. Thus $\mathrm{per}_A(P) = |\mathrm{Orb}_A(P)|$.

Lemma 3.2. *Let N be a positive integer. Then, A^k fixes $(0,1)$ modulo N if and only if $A^k = \mathsf{Id}$ in $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$. Thus, the Pisano period coincides with* $\mathrm{per}_A(P_N)$ *and* $\mathrm{ord}_A(N)$*. Moreover,* $\mathrm{ord}_A(2) = 3$ *and* $\mathrm{ord}_A(N)$ *is even if $N \geq 3$.*

The period of F_k divides the period of A. Now, if (F_k) has period q modulo N, then $(F_q, F_{q+1}) = (0,1)$; this implies $A^q(0,1) = (0,1)$ modulo N. Then, $A^q A(0,1) = A(0,1) = (1,1)$ and we conclude that $A^q A = A$.

Proof. If $A^k = \mathsf{Id}$ in $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$ then, of course, A^k fixes $(0,1)$ and (F_n) is k-periodic modulo N. For the converse, assume that modulo N we have

$$A^k \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \text{i.e.} \quad \begin{pmatrix} F_k \\ F_{k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.4}$$

By definition of the Fibonacci sequence, $A^{k+1} = A$ modulo N, and thus $A^k = \mathsf{Id}$. The last assertion follows from $\det(A) = -1$, which forces $\mathrm{ord}_A(N)$ to be even if $N \geq 3$. □

We have

$$\mathrm{per}_A(Q_N)|\mathrm{per}_A(P_N) = \mathrm{ord}_A(N). \tag{3.5}$$

Indeed, η projects the orbit of P_N under f_A to the orbit of $\eta(P_N)$ in $\mathbf{R}^2/L_G$ under g_A, and this second orbit is identified to the orbit of Q_N under f_A by the conjugacy h_C.

Theorem 3.3. *If $N = 5F_k$ with $k \geq 2$, then*

$$\mathrm{per}_A(Q_N) = 4k \quad \textit{if } k \textit{ is odd},$$
$$\mathrm{per}_A(Q_N) = 2k \quad \textit{if } k \textit{ is even}.$$

Example 3.4. Take $k = 2$, so that $5F_k = 5$. Then $\mathrm{per}_A(Q_5) = 4$; indeed, the f_A-orbit of period 4 is exactly the orbit of Q_5. More precisely, A has 3 orbits in $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$; they correspond to the following orbits of f_A in $(\frac{1}{5}\mathbf{Z}^2)/L$: The fixed point O; the orbit of period 4, $\{f_A^n(Q_5); n \in \mathbf{Z}/4\mathbf{Z}\}$; an orbit of period 20, namely $\{f_A^n(P_5); n \in \mathbf{Z}/20\mathbf{Z}\}$. In particular, $\mathrm{ord}_A(5) = 20$.

Example 3.5. For $k = 3$, $5F_3 = 10$, and one easily checks that $\mathrm{per}_A(Q_{10}) = 12$ and $\mathrm{ord}_A(10) = \mathrm{per}_A(P_{10}) = 60$. See Figure 1.

To prove Theorem 3.3, let us decompose the initial vectors $(F_0, F_1) = (0,1)$ and $(L_0, L_1) = (2,1)$ in a basis of eigenvectors. The eigenlines of A are $E_+ = \mathbf{R}v_+$, with eigenvalue φ, and $E_- = \mathbf{R}v_-$, with eigenvalue φ', where

$$v_+ = \begin{pmatrix} 1 \\ \varphi \end{pmatrix}, \quad v_- = \begin{pmatrix} 1 \\ \varphi' \end{pmatrix}. \tag{3.6}$$

We obtain $(0,1) = \frac{1}{\sqrt{5}}(v_+ - v_-)$, $(2,1) = v_+ + v_-$, and then

$$A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi^n - (\varphi')^n \\ \varphi^{n+1} - (\varphi')^{n+1} \end{pmatrix} \tag{3.7}$$

$$A^n \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} L_n \\ L_{n+1} \end{pmatrix} = \begin{pmatrix} \varphi^n + (\varphi')^n \\ \varphi^{n+1} + (\varphi')^{n+1} \end{pmatrix} \tag{3.8}$$

or equivalently $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (\varphi')^n)$ and $L_n = \varphi^n + (\varphi')^n$.

Proof of Theorem 3.3. From Example 3.4, we can and do assume $k \geq 3$.

Let N be a positive integer. Using $\varphi^{-1} = -\varphi'$ we get, for $n \in \mathbf{Z}$,

$$A^n(Q_N) = \frac{1}{N}\left(\varphi^n v_+ + (\varphi')^n v_-\right) \tag{3.9}$$

$$A^{-n}(Q_N) = \frac{(-1)^n}{N}\left((\varphi')^n v_+ + \varphi^n v_-\right) \tag{3.10}$$

Thus,

$$A^n(Q_N) - (-1)^n A^{-n}(Q_N) = \frac{5F_n}{N}\begin{pmatrix}0\\1\end{pmatrix} \tag{3.11}$$

for every $n \in \mathbf{Z}$.

We first prove that if $N = 5F_k$, the period $m = \mathrm{per}_A(Q_N)$ satisfies $m > k$. Indeed, we have by definition $A^m(Q_N) - Q_N \in L$ so its first coordinate $(L_m - 2)/(5F_k)$ must be a positive integer. Notice that for all $n \geq 1$, we have $L_n < 5F_n$; indeed this is true for $n = 1, 2$ and both sides satisfy the same recursion. Hence $1 \leq (L_m - 2)/(5F_k) < F_m/F_k$, so $m > k$.

Let us assume now that $N = 5F_k$ for some even $k > 2$; write $k = 2\ell$. From Equation (3.11) we obtain $A^k(Q_N) = A^{-k}(Q_N)$ modulo L, which implies that $f_A^{2k}(Q_N) = Q_N$ in $\mathbf{R}^2/L$ and m divides $2k$. Since $m > k$, $m = 2k$.

Now, suppose that $N = 5F_k$ for some odd $k > 2$. From Equation (3.11) we obtain $A^k(Q_N) + A^{-k}(Q_N) \in L$, which implies $f_A^{2k}(Q_N) = -Q_N \mod (L)$; thus, m divides $4k$, and $m > k$, so the remaining possibilities for m are $2k$, $4k/3$ and $4k$. The order is not equal to $2k$ because $-Q_N \neq Q_N$. To conclude that $m = 4k$, it remains to exclude the possibility $k = 3\ell$, $m = 4\ell$ for some $\ell \in \mathbf{N}^*$. But in this case, k and thus ℓ being odd, the equation $f_A^m(Q_N) = Q_N$ implies that $A^{2\ell}Q_N - A^{-2\ell}Q_N$ is an integral point. We conclude from the fact that the second coordinate is $F_{2\ell}/F_{3\ell}$, which is not an integer because $\ell > 0$. □

Theorem 3.6. *If $N = 5F_k$ with $k \geq 2$, then* $\mathrm{per}_A(P_N) = 5\mathrm{per}_A(Q_N)$. *Thus,*

$$\mathrm{per}_A(P_N) = \mathrm{ord}_A(N) = 20k \quad \textit{if } k \textit{ is odd},$$
$$\mathrm{per}_A(P_N) = \mathrm{ord}_A(N) = 10k \quad \textit{if } k \textit{ is even}.$$

Remark 3.7. Modulo 5, the Lucas sequence 2, 1, 3, 4, 2, 1, ... is periodic of period 4 and does not vanish.

Proof. Let m be the period of Q_N under f_A; this is also the period of $\eta(P_N)$ under g_A. Thus, $f_A^m(P_N) = P_N + W$ for some $W \in G$. Our first remark is that $W \neq 0$ or, equivalently, $A^m(P_N) \neq P_N \mod (L)$. Indeed,

$$A^m(P_N) = \frac{1}{N}\begin{pmatrix}F_m\\F_{m+1}\end{pmatrix}. \tag{3.12}$$

If k is even, $m = 2k$, and the first coordinate is

$$\frac{F_{2k}}{5F_k} = \frac{1}{5}\frac{\varphi^{2k} - (\varphi')^{2k}}{\varphi^k - (\varphi')^k} = \frac{L_k}{5} \tag{3.13}$$

but this is never an integer because L_k is never divisible by 5 (see Remark 3.7). Since the first coordinate of P_N is 0, this shows that $A^m(P_N) \neq P_N \mod (L)$. If k is odd, $m = 4k$, and the first coordinate of $A^m(P_N)$ is

$$\frac{F_{4k}}{5F_k} = \frac{1}{5}\frac{\varphi^{4k} - (\varphi')^{4k}}{\varphi^k - (\varphi')^k} = \frac{L_k L_{2k}}{5}. \tag{3.14}$$

By Remark 3.7 again, $L_k L_{2k} \neq 0 \mod (5)$ and $A^m(P_N) \neq P_N \mod (L)$.

Thus, $\mathrm{per}_A(P_N) > \mathrm{per}_A(Q_N)$. On the other hand, a simple recursion shows that

$$f_A^{mn}(P_N) = P_N + W + f_A^m(W) + \cdots + f_A^{m(n-1)}(W) \tag{3.15}$$

for all $n \geq 1$. We know from Section 3.1 that, if we identify G to $\mathbf{Z}/5\mathbf{Z}$, then f_A acts on G as multiplication by 3; since $4|m$ and $3^4 = 1 \mod (5)$, we get $(f_A^m)_{|G} = \mathrm{Id}_{|G}$. Thus, $f_A^{5m} = P_N + 5W = P_N$ and $\mathrm{per}_A(P_N)|5m$. Since 5 is prime, $m|\mathrm{per}_A(P_N)$ and $\mathrm{per}_A(P_N) > m$, we obtain $\mathrm{per}_A(P_N) = 5m$. □

Remark 3.8. Theorem 3.6 provides a sequence of integers $N(\ell) = 5F_{2\ell+1}$ for which $\mathrm{ord}_A(N(\ell)) = 40\ell + 20$; asymptotically,

$$\mathrm{ord}_A(N(\ell)) \simeq \frac{20}{\log(\varphi)}\log(N(\ell)) \simeq (95.7...)\log(N(\ell)). \tag{3.16}$$

For $N(\ell) = 5F_{2\ell}$ we get $\mathrm{ord}_A(N(\ell)) \simeq \frac{10}{\log(\varphi)}\log(N(\ell))$. As we shall see in Section 4.2, this is an unusually small order.

3.4. **The farfalle.** The proof of Theorem 3.3 contains all the necessary ingredients to prove the following result.

Theorem 3.9. *Fix a real number $\varepsilon \in]0,1[$. If $N = 5F_k$ for some $k \geq 2$, then*

$$\frac{|\{P \in \mathrm{Orb}_A(Q_N)\ ;\ \mathrm{dist}(O,P) \leq \varepsilon\}|}{|\mathrm{Orb}_A(Q_N)|} \geq 1 - \left\lceil 1 - \frac{\log(\varepsilon/\sqrt{2})}{\log(\varphi)} \right\rceil \frac{1}{k}.$$

Thus, as k increases, most of the orbit of Q_N stays near the origin O.

Proof. The f_A-orbit of Q_N corresponds to the sequence of points

$$A^n(Q_N) = \frac{1}{N}(\varphi^n v_+ + (\varphi')^n v_-) = \frac{1}{5F_k}\begin{pmatrix} L_n \\ L_{n+1} \end{pmatrix} \tag{3.17}$$

with $n \in \mathbf{Z}$; to describe the full orbit, we can restrict to $n \in \{0,1,2,\ldots,\mathrm{per}_A(Q_N) - 1\}$ or to $n \in \{-\mathrm{per}_A(Q_N)/2, \ldots, \mathrm{per}_A(Q_N)/2\}$ (the period is always even). If

$n \geq 0$, then

$$\frac{L_n}{5F_k} = \frac{1}{\sqrt{5}} \frac{\varphi^n + (\varphi')^n}{\varphi^k - (\varphi')^k} \tag{3.18}$$

$$= \frac{1}{\varphi^{k-n}} \frac{1}{\sqrt{5}} \frac{1 + (-(\varphi')^2)^n}{1 + (-(\varphi')^2)^k} \tag{3.19}$$

$$\leq \frac{1}{\varphi^{k-n}}. \tag{3.20}$$

Similarly

$$\frac{|L_{-n}|}{5F_k} = \frac{|\varphi'|^{-n}}{\varphi^k} \frac{1}{\sqrt{5}} \frac{1 + (-(\varphi)^2)^{-n}}{1 + (-(\varphi')^2)^k} \leq \frac{1}{\varphi^{k-n}}. \tag{3.21}$$

If k is even, $\mathrm{per}_A(Q_N) = 2k$, and taking n in $\{-k, \ldots, k\}$ we cover the full orbit of Q_N. If we restrict to $n \in \{-k+\ell, \ldots, k-\ell\}$ with $\ell \in \mathbf{N}$ such that

$$\frac{1}{\varphi^{\ell-1}} \leq \frac{\varepsilon}{\sqrt{2}} \tag{3.22}$$

then the corresponding points $f_A^n(Q_N)$ are at (eudlidean) distance $\leq \varepsilon$ from the origin O in $\mathbf{R}^2/L$. This amounts to choose

$$\ell \geq 1 - \frac{\log(\varepsilon/\sqrt{2})}{\log(\varphi)}. \tag{3.23}$$

Optimizing the choice of ℓ, we obtain the result stated in the theorem.

If k is odd then $\mathrm{per}_A(Q_N) = 4k$, and we know from the proof of Theorem 3.3 that $f_A^k(Q_N) = -f_A^{-k}(Q_N)$. Thus, the norm of $f_A^n(Q_N)$ is in fact periodic of period $2k$, and the same argument applies. □

Corollary 3.10. *Fix a real number $\varepsilon \in]0,1[$. If $N = 5F_k$ for some $k \geq 2$, then*

$$\frac{|\{P \in \mathrm{Orb}_A(P_N)\ ;\ \mathrm{dist}(G,P) \leq \varepsilon\}|}{|\mathrm{Orb}_A(P_N)|} \geq 1 - \left\lceil 1 - \frac{\log(\varepsilon/\sqrt{2})}{\log(\varphi)} \right\rceil \frac{1}{k}.$$

This follows directly from the last theorem, and the fact that the linear map C used to conjugate the dynamics of f_A to the dynamics of g_A has norm ≤ 1.

Proof of Theorem A. Set $G^* = G \setminus \{O\}$. The last corollary shows that for $N = 5F_k$, most of the orbit of P_N stays close to G. And when a point P of the orbit is close to some $g \in G^*$ then the next four points $f_A^i(P)$, $1 \leq i \leq 4$, circle around G^* in the order of the farfalle.

To conclude, we have to show that for any $g \in G$, the proportion of points in $\mathrm{Orb}_A(P_N)$ near g is close to $1/5$, up to an error bounded by $\left\lceil 1 - \frac{\log(\varepsilon/\sqrt{2})}{\log(\varphi)} \right\rceil \frac{1}{k}$.

To explain this phenomenon, assume that k is even, so that $\mathrm{per}_A(Q_N) = 2k$. Recall from the proof of Theorem 3.6 that $f^{2kq}(P_N) = P_N + qW$, for some $W \in G^*$ and all $q \in \mathbb{N}$. Then, choose on optimal ℓ that satisfies Equation (3.23). For n between $-k+\ell$ and $k-\ell$ the points $f_A^n(P_N)$ are close to the origin. Then $f_A^{2k+n}(P_N) = f_A^n(P_N) + f_A^n(W)$ where $f_A^n(W)$ describes G^* periodically with period 4. Thus, for each $g \in G^*$, $1/4$ of these $2k-2\ell+1$ points $f_A^{2k+n}(P_N)$ are close to g. The same phenomenon occurs when we apply f_A^{4k}, f_A^{6k}, f_A^{8k}, so the amount of time spent by the orbit of P_N near $g \in G$ does not depend on g. The proof with odd k is similar. □

4. Intermezzo I: Periods of the Fibonacci sequence

We collect a few basic facts on the period of the Fibonacci matrix modulo N and state some advanced results due to Kurlberg and Rudnick.

4.1. **Periods.**

4.1.1. *The golden mean.* The (complex) eigenvalues of A are φ and its Galois conjugate $\varphi' = -1/\varphi$; they are roots of

$$t^2 = t + 1. \tag{4.1}$$

They live in the quadratic extension $\mathbf{Q}[\sqrt{5}]$, $\mathbf{Z}[\varphi]$ is the ring of integers of $\mathbf{Q}[\sqrt{5}]$, and -1 and φ generate the (multiplicative) group of units. Now, fix a prime $p \neq 2, 5$, and consider the Equation (4.1) over the finite field $\mathbf{F}_p$, keeping the same notation $\{\varphi, \varphi'\}$ for its roots. The quadratic reciprocity says that

- $\{\varphi, \varphi'\} \subset \mathbf{F}_p$ if and only if 5 is a square modulo p, if and only if p is a square modulo 5, if and only if $p = 1$ or $4 \mod (5)$;
- otherwise, φ, φ' live in the quadratic extension $\mathbf{F}_p[t]/(t^2-t-1) \simeq \mathbf{F}_{p^2}$.

For $\lambda \in \mathbf{F}_p^*$, we denote its multiplicative order by $\mathrm{ord}_\lambda(p)$; thus $\mathrm{ord}_\lambda(p) | (p-1)$. When 5 is a square modulo p, *we always choose* φ *and* φ' *such that* $\mathrm{ord}_{\varphi'}(p) \geq \mathrm{ord}_\varphi(p)$; then, two cases are possible:

- $\mathrm{ord}_\varphi(p) = 1 \mod (2)$ and $\mathrm{ord}_{\varphi'}(p) = 2\mathrm{ord}_\varphi(p)$;
- $\mathrm{ord}_\varphi(p) = 0 \mod (4)$ and $\mathrm{ord}_{\varphi'}(p) = \mathrm{ord}_\varphi(p)$.

Indeed, if $\mathrm{ord}_\varphi(p) = 2\ell$ then $\varphi^\ell = -1$ and $(\varphi')^\ell = (-\varphi)^{-\ell} = -(-1)^\ell$; this implies that ℓ is even, because otherwise $\mathrm{ord}_{\varphi'}(p) = \ell$ would be less than $\mathrm{ord}_\varphi(p)$. Note that this convention impose a clear distinction between φ and φ' only when $\{\varphi, \varphi'\} \subset \mathbf{F}_p$, $\mathrm{ord}_\varphi(p)$ is odd, and $\mathrm{ord}_{\varphi'}(p) = 2\mathrm{ord}_\varphi(p)$ (the statements to come will be symmetric in φ and φ' in all other cases).

4.1.2. *Order of A, order of* φ*, orbit periods.* When 5 is a square modulo p, then A is diagonalisable over $\mathbf{F}_p$; we denote by $E(p)$ and $E'(p)$ the eigenlines of A in $\mathbf{F}_p^2$ corresponding to φ and φ' respectively. Then, the orders of A in $\mathsf{GL}_2(\mathbf{F}_p)$ and of φ in $\mathbf{F}_p^*$ satisfy

$$\mathrm{ord}_A(p) = 2\mathrm{ord}_\varphi(p) \quad \text{if} \quad \mathrm{ord}_\varphi(p) = 1 \mod (2), \tag{4.2}$$

$$\mathrm{ord}_A(p) = \mathrm{ord}_\varphi(p) \quad \text{if} \quad \mathrm{ord}_\varphi(p) = 0 \mod (4). \tag{4.3}$$

When 5 is not a square modulo p, $\mathrm{ord}_A(p)$ equals the order of φ in $\mathbf{F}_{p^2}^\times$.

Proposition 4.1. *If* 5 *is not a square modulo p, then* $\mathrm{per}_A(P) = \mathrm{ord}_A(p)$ *for every* $P \neq O$ *in* $\mathbf{F}_p^2$*, and* $\mathrm{ord}_A(p)$ *is equal to the order of* φ *(and of* φ'*) in the multiplicative group* $\mathbf{F}_{p^2}^\times$.

If 5 *is a square modulo p, we have the following possible periods*

- *if* $\mathrm{ord}_\varphi(p) = 1 \mod (2)$*, then* $\mathrm{per}_A(P) = \mathrm{ord}_\varphi(p) = \mathrm{ord}_A(p)/2$ *if P is in* $E(p) \setminus \{O\}$ *and* $\mathrm{per}_A(P) = 2\mathrm{ord}_\varphi(p) = \mathrm{ord}_A(p)$ *if P is in* $\mathbf{F}_p^2 \setminus E(p)$*;*
- *if* $\mathrm{ord}_\varphi(p) = 0 \mod (4)$*, then* $\mathrm{per}_A(P) = \mathrm{ord}_\varphi(p) = \mathrm{ord}_A(p)$ *for every* $P \neq O$ *in* $\mathbf{F}_p^2$.

Proof. Suppose that 5 is not a square modulo p. Then, φ' is the Galois conjugate of φ in the quadratic extension $\mathbf{F}_{p^2}$, so that the orders of φ' and of φ in $\mathbf{F}_{p^2}^\times$ are equal. Since A is conjugate to the diagonal matrix with eigenvalues φ and φ', the order of A in $\mathsf{GL}(\mathbf{F}_p)$ and in $\mathsf{GL}(\mathbf{F}_{p^2})$ is equal to the order of φ in $\mathbf{F}_{p^2}^\times$. Now, fix a point P in $\mathbf{F}_p^2$ and set $k = \mathrm{per}_A(P)$. Then, k divides $\mathrm{ord}_A(p)$. Writing $P = (x,y)$ in a basis in which A is diagonal, we obtain $(\varphi^k x, (\varphi')^k y) = (x,y)$; since x or y is non-zero, we deduce that the order of φ divides k. Thus, $k = \mathrm{ord}_A(p)$.

When 5 is a square modulo p, the argument is similar, but slightly more involved. We leave it to the reader. □

As a consequence $\mathrm{per}_A(P) = \mathrm{ord}_A(p)$ for every $P \neq O$ except when $p = 1$ or $4 \mod (5)$, $\mathrm{ord}_\varphi(p)$ is odd, and P is in $E(p)$. Also, the period of $(0,1) \in \mathbf{F}_p^2$ is equal to $\mathrm{ord}_A(p)$ for every prime, including $p = 2,5$ (they were excluded to streamline the expositon, because $1 = -1 \mod (2)$ and $t^2 - t - 1 = (t-3)^2 \mod (5)$); this fact holds modulo any integer N, see Lemma 3.2.

Example 4.2. Consider the prime $p = 143287$. It is equal to 2 modulo 5. The order of A modulo p divides $p^2 - 1$ and is in fact equal to $2(p+1) = 286576$.

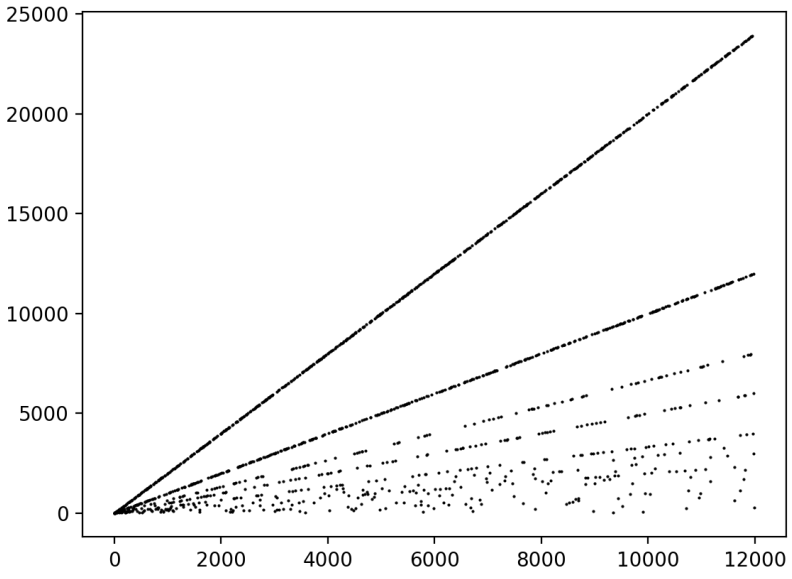

FIGURE 5. Order of the Fibonacci matrix A modulo primes between 1 and 12000.

4.2. **Pisano sequence, Artin's conjecture, and lower estimates of the periods.** By definition the period of the Fibonacci sequence taken modulo N, for $N \in \mathbf{N}^*$, is the N-th **Pisano period** and is often denoted $\pi(N)$; it's equal to the order $\mathrm{ord}_A(N)$ (see Lemma 3.2). Not much is known on $(\pi(N))$, even when one restricts to prime values of N. Here is a sample of results:

(1) one always has $\pi(N) \leq 6N$, with equality if and only if $N = 2 \times 5^k$ for some $k \geq 1$ (see [5]);
(2) if p is a prime, then $\mathrm{ord}_A(p^k) \simeq c_p p^k$ for large values of k and a fixed c_p (to see this, write $A^r = \mathsf{Id} + p^\ell B$ where r is the order of A modulo p and B is not zero modulo p, then expand $(A^r)^k = \mathsf{Id} + kp^\ell B + p^{2\ell}...$; see [11, Theorem 5]);
(3) more generally, by the chinese remainder theorem, $\mathrm{ord}_A(N^k) \gtrsim N^k$ for large values of k if $N \geq 2$.
(4) for every N, $\mathrm{ord}_A(N) \geq \log(N)/\log(2)$, because the norm of A with respect to the ℓ^∞-norm is equal to 2, so all coefficients of A^k are positive integers in $\{1,\ldots,N-1\}$ if $1 < k\log(2) < \log(N)$.

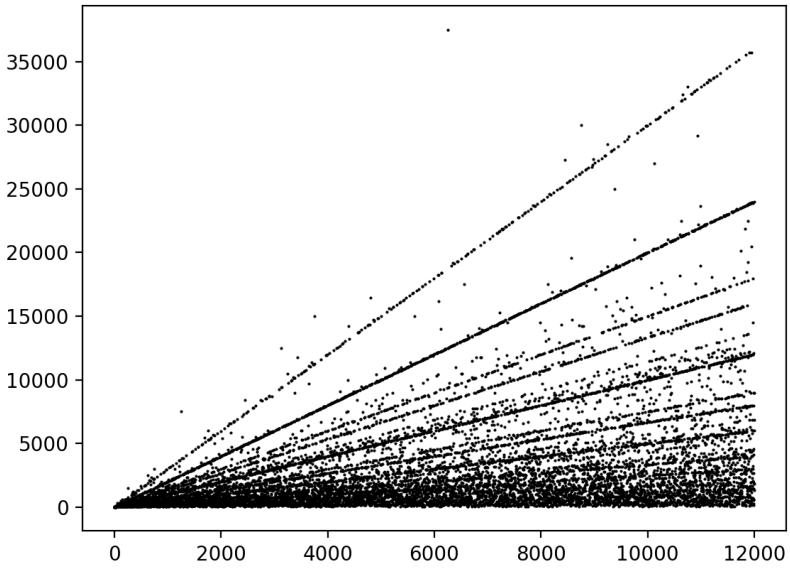

FIGURE 6. Order of the Fibonacci matrix A modulo integers between 1 and 12000. The point $(6250, 37500)$ illustrates the first assertion in Section 4.2, since $6250 = 2 \times 5^5$.

Of interest to us, is the question of determining integers N for which $\mathrm{ord}_A(N)$ is of the order of magnitude of N, as in the first three assertions. This is a delicate question, similar to the following famous conjecture of Artin: *Let a be an integer which is not a perfect square nor -1; then, the multiplicative order of a modulo p is equal to $p-1$ (equivalently, a generates the multiplicative group $\mathbf{F}_p^\times$) for a set of primes of positive relative density*. The following elementary Lemma will be too weak for our main results, but it applies to most primes. We include a short proof for completeness (see [3] and [8, Lemma 15]).

Lemma 4.3. *The set of primes p such that $\mathrm{ord}_A(p) \geq p^{1/2}/\log(p)$ is of full relative density among all primes.*

Proof. Consider the set $\mathcal{P}(x)$ of primes $p \leq x$ such that $F_k = 0 \mod (p)$ for some $0 < k \leq p^{1/2}/\log(p)$. Then

$$|\mathcal{P}(x)| \leq \sum_{k=1}^{x^{1/2}/\log(x)} \omega(F_k) \tag{4.4}$$

where $\omega(N)$ denotes the number of distinct prime factors of N. Since $\omega(N) \leq \log(N)$ for $N \geq 7$ and $\sqrt{5}F_k \leq \varphi^k$, one easily gets

$$|\mathcal{P}(x)| \leq \frac{\log(\varphi)}{2} \frac{x}{(\log(x))^2}. \tag{4.5}$$

The prime number theorem shows that the proportion of primes $\leq x$ in $\mathcal{P}(x)$ converges towards 0 as x goes to $+\infty$. □

Theorem 4.4 (Kurlberg Rudnick, [8, Theorem 17])**.** *There is a positive constant* δ *and a subset* K *of* $\mathbf{N}^*$ *of density* 1 *such that*

$$\mathrm{ord}_A(N) \gtrsim \sqrt{N}\exp(\log(N)^\delta)$$

for all N *in* K.

The first step in the proof of this result states that for each $1/2 < \eta < 3/5$, there is a set of primes K_η of relative density $c(\eta) = \frac{1}{2}(3-5\eta)/(1-\eta)$ such that $\mathrm{ord}_A(p) \gtrsim p^\eta$ for all p in K_η. If one adds the constraint $p = a \mod (5)$ for some invertible $a \in \mathbf{Z}/5\mathbf{Z}$, then the proof provides a set of primes $K_\eta(a)$ of density $c(\eta)/4$ among all primes (here, 4 is the number of invertible elements in $\mathbf{Z}/5\mathbf{Z}$): See the Equation (6.2) at the beginning of Section 6.1 in [8].

Corollary 4.5 (of the proof of Theorem 4.4)**.** *For any* $\varepsilon > 0$ *, the set of primes* p *such that* 5 *is not a square modulo* p *(resp. is a square modulo* p*) and* $\mathrm{ord}_A(p) \geq p^{\frac{3}{5}-\varepsilon}$ *has positive relative density among all primes.*

Remark 4.6. Assuming the generalized Riemann hypothesis (GRH), Kurlberg proved the following result in [7]: *If* $\tau\colon \mathbf{R}_+ \to \mathbf{R}_+$ *is an increasing function tending to infinity more quickly than the logarithm, the set of primes* p *such such* $\mathrm{ord}_B(p) \geq p/\tau(p)$ *has density* 1. Since roughly $1/2$ of the primes are equal to 2 or 3 modulo 5, Corollary 4.5 holds (under GRH) for a set of primes of relative density $1/2$, the maximum one can hope for. Kurlberg also obtains the following improvement of Theorem 4.4: *Assuming GRH, there is a set* $K' \subset \mathbf{N}^*$ *of density* 1 *such that* $\mathrm{ord}_A(N) \gtrsim N^{1-\varepsilon}$ *for* N *in* K_ε.

5. When the farfalle disappears: Entropy estimate

In this section, following [2]*, ideas from ergodic theory are used to control the complexity of periodic orbits of the Fibonacci transformation* f_A*. The main ingredients are metric entropy and uniform hyperbolicity.*

5.1. **Entropy.** Let X be a compact, metric space, and let f be a homeomorphism of X. Let μ be a probability measure on X. Recall that μ is f-invariant if $\mu(f^{-1}(B)) = \mu(B)$ for every Borel set $B \subset X$.

5.1.1. *Metric entropy.* Let $\mathcal{P} = \{A_i \; ; \; i = 1, \ldots, \ell(\mathcal{P})\}$ be a partition of X into finitely many Borel subsets $A_i \subset X$, called the atoms of $\mathcal{P}$. The pull-back of $\mathcal{P}$ by f is the partition $f^{-1}\mathcal{P} = \{f^{-1}(A_i) \; ; \; A_i \in \mathcal{P}\}$. By definition, the entropy $H_\mu(\mathcal{P})$ of $\mathcal{P}$ for μ is

$$H_\mu(\mathcal{P}) = \sum_{A_i \in \mathcal{P}} -\mu(A_i) \log(\mu(A_i). \tag{5.1}$$

If μ is f-invariant, then $H_\mu(f^{-1}\mathcal{P}) = H_\mu(\mathcal{P})$.

The join of two finite partitions $\mathcal{P}$ and $\mathcal{P}'$ is the partition obtained by intersecting the atoms of $\mathcal{P}$ and $\mathcal{P}'$: $\mathcal{P} \vee \mathcal{P}' = \{A_i \cap A'_j \; ; \; 1 \leq i \leq \ell(\mathcal{P}), 1 \leq j \leq \ell(\mathcal{P}'), A_i \cap A'_j \neq \emptyset\}$. The join of finitely many partitions is defined similarly. There is a sub-additivity property of the entropy, namely

$$H_\mu(\mathcal{P} \vee \mathcal{P}') \leq H_\mu(\mathcal{P}) + H_\mu(\mathcal{P}'), \tag{5.2}$$

as well as a monotony property, which means that

$$H_\mu(\mathcal{P}) \leq H_\mu(\mathcal{P}') \tag{5.3}$$

if the partition $\mathcal{P}'$ is finer than $\mathcal{P}$.

Now, assume that the measure μ is f-invariant. The entropy of μ with respect to f and to the starting partition $\mathcal{P}$ is

$$h_\mu(f; \mathcal{P}) = \lim_{n \to +\infty} \frac{1}{n} H_\mu \left(\bigvee_{i=0}^{n-1} f^{-i}\mathcal{P} \right), \tag{5.4}$$

where the existence of the limit follows from the sub-additivity (5.2); moreover, this limit is in fact an infimum. The entropy of μ is $h_\mu(f) = \sup_{\mathcal{P}} h_\mu(f; \mathcal{P})$ where the supremum is taken over all such finite partitions. Note that, from the invariance of μ, we can replace $\bigvee_{i=0}^{n-1} f^{-i}\mathcal{P}$ by $\bigvee_{i=-k}^{n-k-1} f^{-i}\mathcal{P}$ in the definition of $h_\mu(f; \mathcal{P})$, this for any k (depending on n or not).

If the limit of $\bigvee_{i=-n}^{n} f^{-i}\mathcal{P}$, as n goes to $+\infty$, is the partition into points, one says that $\mathcal{P}$ is a generating partition for the dynamics of f. In that case, the Kolmogorov-Sinai Theorem tells us that $h_\mu(f) = h_\mu(f; \mathcal{P})$.

5.1.2. *Entropy, dimension comparison.* Let $Y \subset X$ be compact. Fix an $\varepsilon > 0$, and consider the minimal number $\mathrm{Cov}_\varepsilon(Y)$ of subsets of X of diameter $\leq \varepsilon$ needed to cover Y. Typically, $\mathrm{Cov}(\varepsilon)$ grows like a power of $1/\varepsilon$, thus one sets

$$\dim_B^-(Y) = \liminf_{\varepsilon \to 0} \frac{\log(\mathrm{Cov}_\varepsilon(Y))}{\log(1/\varepsilon)}. \tag{5.5}$$

This is the lower box dimension of Y. The following result is well-known.

Theorem 5.1 (see [9])**.** *Assume that $f\colon X \to X$ is Lipschitz, with Lipschitz constant* $\mathrm{Lip}(f)$*. Then,*

$$h_\mu(f) \leq \dim_B^-(\mathrm{Supp}(\mu)) \times \log(\mathrm{Lip}(f))$$

where $\mathrm{Supp}(\mu)$ *is the support of* μ*.*

5.2. **Automorphisms of the torus.** Endow $\mathbf{R}^2/\mathbf{Z}^2$ with the euclidean distance dist. Let $f_B\colon \mathbf{R}^2/\mathbf{Z}^2 \to \mathbf{R}^2/\mathbf{Z}^2$ be a linear Anosov diffeomorphism, induced by an element B of $\mathsf{GL}_2(\mathbf{Z})$ whose eigenvalues λ and λ' satisfy $|\lambda| > 1 > |\lambda'|$ (note that $\lambda' = \det(B)\lambda^{-1} = \pm\lambda^{-1}$). Fix a basis of unit eigenvectors w^+ and w^- for B, with $Bw^+ = \lambda w^+$, $Bw^- = \lambda' w^-$. If Q is a point of $\mathbf{Q}^2/\mathbf{Z}^2$, we denote by $\mathrm{per}_B(Q)$ the period of Q under the action of f_B. Let μ be any f_B-invariant probability measure.

1.- If $\mathcal{P}$ is a partition of $\mathbf{R}^2/\mathbf{Z}^2$ which is made of rectangles, the sides of which are parallel to w^+ and w^-, and if the rectangles are small enough, then $\mathcal{P}$ is a generating partition for f_B. Thus, $h_\mu(f_B) = h_\mu(f_B; \mathcal{P})$.

2.- f_B is $|\lambda|$-Lipschitz, thus $h_\mu(f) \leq \dim_B^-(\mathrm{Supp}(\mu)) \times \log(|\lambda|)$. In fact, in this setting, the Hausdorff dimension, lower box dimension, and upper box dimension of $\mathrm{Supp}(\mu)$) coincide (see [12, §4]).

5.3. **Entropy estimate from arithmetic dispersion.** In the following theorem, which is directly inspired by the work of Einsiedler, Lindenstrauss, Michel, and Venkatesh (see [2], Section 4.2), B is as in the previous paragraph.

Theorem 5.2. *Let ε be a positive real number. Let (Q_k) be a sequence of rational points in $\mathbf{R}^2/\mathbf{Z}^2$ such that*

(i) $\lim N_k = +\infty$*, where N_k is the order of Q_k in $\mathbf{R}^2/\mathbf{Z}^2$, i.e. N_k is the least positive integer such that $N_k Q_k = 0 \mod \mathbf{Z}^2$;*
(ii) $\mathrm{per}_B(Q_k) \geq N_k^\varepsilon$*;*

(iii) *the sequence of probability measures*

$$\mu_k = \frac{1}{\mathrm{per}_B(Q_k)} \sum_{i=0}^{\mathrm{per}_B(Q_k)-1} \delta_{f_B^i(Q_k)}$$

converges towards some measure μ.

Then, the entropy of μ is bounded from below by $\frac{\varepsilon}{2}\log(|\lambda|)$.

Remark 5.3. Note that N_k is the smallest integer such that $Q_k \in \frac{1}{N_k}\mathbf{Z}^2 \mod \mathbf{Z}^2$; thus, N_k can be considered as the arithmetic complexity of Q_k (it is the multiplicative height of the lift of Q_k to $\mathbf{R}^2$ with coordinates between 0 and 1).

Proof. Fix a basis of unit eigenvectors w^+, w^-, as in Section 5.2. In this proof, we use the distance dist_∞ induced by the sup-norm with respect to this basis. Thus, a set has diameter $\leq D$ if it can be included in a parallelogram, the sides of which are parallel to w^+ and w^- and have length at most D. There is a constant $C > 1$ such that

$$C^{-1}\mathrm{dist}_\infty(q,q') \leq \mathrm{dist}(q,q') \leq C\mathrm{dist}_\infty(q,q') \tag{5.6}$$

for all pairs of points q, q'. Thus, a set of diameter $< \frac{1}{CN_k}$ for dist_∞ contains at most one point with coordinates in $\frac{1}{N_k}\mathbf{Z}^2$.

Let $\mathcal{P}$ be a finite partition of the torus by atoms A_i of diameter $\mathrm{diam}(A_i) < R := C^{-1}$. Let m_0 be a positive integer. Our ultimate goal is the inequality

$$\frac{1}{2m_0} H_\mu(\bigvee_{i=0}^{2m_0} f_B^{-i}\mathcal{P}) \geq \frac{\varepsilon}{2}\log|\lambda|. \tag{5.7}$$

Indeed, if we prove this inequality for every m_0, then taking a limit as m_0 increases to $+\infty$, and using the sub-additivity of the entropy (Equation (5.2)), we deduce that $h_\mu(f_B) \geq \frac{\varepsilon}{2}\log|\lambda|$, as desired.

Note that, because μ is f_B-invariant, the entropy on the left of Equation (5.7) is equal to $H_\mu(\bigvee_{i=-m_0}^{m_0} f_B^{-i}\mathcal{P})$.

Now, consider the partition $\mathcal{P}^{(m)} = \bigvee_{i=-m}^{m} f_B^{-i}\mathcal{P}$ for any $m > 0$. The atoms of $\mathcal{P}^{(m)}$ have diameter bounded from above by $R|\lambda|^{-m}$ ([2]). Thus, we set

$$m_k = \left\lceil \frac{\log(CR) + \log(N_k)}{\log|\lambda|} \right\rceil = \left\lceil \frac{\log(N_k)}{\log|\lambda|} \right\rceil \tag{5.8}$$

[2]Indeed, the A_j are contained in parallelograms whose sides are parallel to w^+ and w^- and have length $\leq R$. Since f_B^i multiplies lengths by $|\lambda|^i$ in the w^+ (resp. w^-) direction if $i \geq 0$ (resp. $i \leq 0$), the atoms of $\mathcal{P}^{(m)}$ are contained in parallelograms of sides $\leq R|\lambda|^{-m}$.

and obtain that the atoms of the partition $\mathcal{P}^{(m_k)}$ have diameter at most $\frac{1}{CN_k}$. In particular, each atom contains at most one point of $\mathbf{R}^2/\mathbf{Z}^2$ with coordinates in $\frac{1}{N_k}\mathbf{Z}^2 \mod \mathbf{Z}^2$.

The measure μ_k is supported on the orbit of Q_k, each point of this orbit is contained in $\frac{1}{N_k}\mathbf{Z}^2 \mod \mathbf{Z}^2$, and the mass of each point is $1/\mathrm{per}_B(Q_k)$. Thus, for the atoms A_i of $\mathcal{P}^{(m_k)}$, we obtain $\mu_k(A_i) = 1/\mathrm{per}_B(Q_k)$ if A_i contains one (and then a unique) point of the orbit, and $\mu_k(A_i) = 0$ otherwise. This gives

$$H_{\mu_k}(\mathcal{P}^{(m_k)}) = \sum_{A_i \in \mathcal{P}^{(m_k)}} -\mu_k(A_i)\log(\mu_k(A_i)) \tag{5.9}$$

$$= \mathrm{per}_B(Q_k)\left(-\frac{1}{\mathrm{per}_B(Q_k)}\log\left(\frac{1}{\mathrm{per}_B(Q_k)}\right)\right) \tag{5.10}$$

$$= \log(\mathrm{per}_B(Q_k)) \tag{5.11}$$

Since $\mathrm{per}_B(Q_k) \geq N_k^{\varepsilon}$, we obtain

$$\frac{1}{2(m_k-1)}H_{\mu_k}(\mathcal{P}^{(m_k)}) \geq \frac{1}{2}\frac{\varepsilon\log|\lambda|\log(N_k)}{\log(N_k)} \tag{5.12}$$

$$= \frac{1}{2}\varepsilon\log|\lambda|. \tag{5.13}$$

To conclude, we derive the lower bound (5.7) from this last inequality. Write the euclidean division of m_k by $2m_0$ as $m_k = q_k 2m_0 + r_k \leq 2(q_k+1)m_0$. Then

$$\mathcal{P}^{(m_k)} \leq \bigvee_{j=-q_k-1}^{q_k+1} f_B^{-j2m_0}\mathcal{P}^{(m_0)}. \tag{5.14}$$

By the monotony and sub-additivity of entropy (see Equations (5.3) and (5.2)), we obtain

$$H_{\mu_k}(\mathcal{P}^{(m_k)}) \leq 2(q_k+1)H_{\mu_k}(\mathcal{P}^{(m_0)}). \tag{5.15}$$

Equations (5.15) and (5.13) imply successively

$$\frac{1}{2m_0}H_{\mu_k}(\mathcal{P}^{(m_0)}) \geq \frac{1}{4(q_k+1)m_0}H_{\mu_k}(\mathcal{P}^{(m_k)}) \tag{5.16}$$

$$\geq \frac{2(m_k-1)}{4(q_k+1)m_0}\frac{1}{2}\varepsilon\log|\lambda| \tag{5.17}$$

and letting $m_k = 2q_k m_0 + r_k$ go to $+\infty$ we obtain the desired Inequality (5.7). This concludes the proof. □

Corollary 5.4. *Under the hypotheses (i) and (ii) of Theorem 5.2, any cluster value μ of the sequence μ_k satisifies*

$$\dim(\mathrm{Supp}(\mu)) \geq \varepsilon,$$

where $\dim(\mathrm{Supp}(\mu))$ *refers equivalently to the Hausdorff, lower box, or upper box dimension of the support of μ.*

Proof. Theorem 5.2, Theorem 5.1, and the results of Section 5.2 give $\varepsilon/2 \leq \dim(\mathrm{Supp}(\mu))$. To get the lower bound stated in the corollary, we refer to a theorem of Lai-Sang Young (see [12, Main Theorem]): $HD(\mu) = \frac{2h_\mu(f_B)}{\log|\lambda|}$, *where $HD(\mu)$ is the smallest Hausdorff dimension of a set of full measure.* □

5.4. **Application.** Consider a sequence of integers (N_k) such that the orbit of $P_k = (0, 1/N_k)$ in $\mathbf{R}^2/L$ under f_A satisfies

$$\mathrm{per}_A(P_k) \geq N_k^\varepsilon. \tag{5.18}$$

Corollary 5.4 provides the following estimate: If the probability measures

$$\mu_k = \frac{1}{\mathrm{per}_A(P_k)} \sum_{n=0}^{\mathrm{per}_A(P_k)-1} \delta_{f_A^n(P_k)}. \tag{5.19}$$

converge towards some measure μ along a subsequence, the Hausdorff dimension of the support of μ is $\geq \varepsilon$. In particular, μ cannot be concentrated on a finite set, as in Launay's farfalle mystery.

5.4.1. *Proof of Theorem B.* According to Theorem 4.4, there is a subset $K \subset \mathbf{N}^*$ of density 1 and a constant $\delta > 0$ such that

$$\mathrm{ord}_A(N) \gtrsim \sqrt{N}\exp((\log(N)^\delta) \tag{5.20}$$

for all N in K. Let (N_k) be an increasing sequence of integers contained in K. From Lemma 3.2 and the Inequality (5.20), the sequence (P_k) satifies the hypotheses (i) and (ii) of Theorem 5.2 with $\varepsilon = 1/2$. Thus, any cluster value μ of (μ_k) satisfies $\dim(\mathrm{Supp}(\mu)) \geq \frac{1}{2}$. This completes the proof of Theorem B.

5.4.2. *Further consequences.* If we consider the sequence $N_k = N^k$ for some fixed $N \geq 2$, we obtain $\dim(\mathrm{Supp}(\mu)) \geq 1$ for any cluster value of μ_k (see § 4.2).

If we restrict to prime numbers, we can apply the lower estimates described at the end of Section 4.2 to get: *For each $1/2 < \eta < 3/5$ there is a set of primes of positive relative density such that if (N_k) is an increasing sequence of such primes and μ is any cluster value of (μ_k), then* $\dim(\mathrm{Supp}(\mu)) \geq \eta$.

Similarly, assuming the generalized Riemann hypothesis, there is a set of integers K_ε (resp. of primes K') of (relative) density 1 such that if (N_k) is an increasing sequence of elements of K_ε (resp. of K') and μ is any cluster value of (μ_k), then $\dim(\mathrm{Supp}(\mu)) \geq (1-\varepsilon)$ (resp. $\dim(\mathrm{Supp}(\mu)) \geq 1$).

6. Intermezzo II: Fourier analysis on finite abelian groups

This section introduces Fourier analysis on finite abelian groups, following the presentation of Tao and Vu in [10].

6.1. **Dual and bilinear forms.** Let $(Z,+)$ be a finite abelian group, with neutral element 0. The (Pontryagin) dual $\hat{Z}$ of Z is the group of all homomorphisms $(Z,+) \to (\mathbf{R}/\mathbf{Z},+)$, the law being addition of homomorphisms; equivalently, this is the group of all homomorphisms $(Z,+) \to (\mathbb{S}^1,\cdot)$ where the law is now provided by multiplication. If Z is the cyclic group $\mathbf{Z}/N\mathbf{Z}$, every homomorphism $\eta\colon Z \to \mathbf{R}/\mathbf{Z}$ is determined by $\eta(1) \in \mathbf{R}/\mathbf{Z}$, with the unique constraint $N\eta(1) = 0$ in $\mathbf{R}/\mathbf{Z}$. Thus, $\hat{Z}$ is isomorphic to the cyclic subgroup $(\frac{1}{N}\mathbf{Z})/\mathbf{Z}$ of $\mathbf{R}/\mathbf{Z}$, hence to Z.

A bilinear form on Z is a map $Z \times Z \to \mathbf{R}/\mathbf{Z}$, $(x,y) \mapsto (x \cdot y)$ which is a homomorphism of abelian groups with respect to each variable separately. It is non-degenerate if for every $z \in Z \setminus \{0\}$ there are elements x and y in Z with $(x \cdot z) \neq 0$ and $(z \cdot y) \neq 0$; otherwise, it is degenerate. It is symmetric if $(x \cdot y) = (y \cdot x)$ for all $(x,y) \in Z^2$.

Consider the map $(x,y) \in \mathbf{Z}^2 \mapsto (x \cdot y) = \frac{1}{N}xy \mod \mathbf{Z}$. Its value at (x,y) depends only on the classes of x and y modulo N; this defines a non-degenerate, symmetric bilinear form on $\mathbf{Z}/N\mathbf{Z}$. If Z_1 and Z_2 are finite abelian groups with symmetric, non-degenerate bilinear forms $(\cdot)_1$ and $(\cdot)_2$, then $((x_1,x_2) \cdot (y_1,y_2)) = (x_1 \cdot y_1)_1 + (x_2 \cdot y_2)_2$ is a symmetric, non-degenerate bilinear form on $Z_1 \times Z_2$. Thus, by the structure of finite abelian groups, each of them admits such a form.

The isomorphism $\widehat{Z_1 \times Z_2} = \hat{Z}_1 \times \hat{Z}_2$ and the isomorphism $\hat{Z} \simeq Z$ for cyclic groups show that $\hat{Z} \simeq Z$ for any finite abelian group. Now, if Z is endowed with a symmetric non-degenerate bilinear form, $k \in Z \mapsto (k\cdot)$ is an isomorphism from Z to $\hat{Z}$; indeed, the non-degeneracy says that this homomorphism is injective, and the equality $|\hat{Z}| = |Z|$ implies that it is bijective.

In what follows, we endow Z with a symmetric, non-degenerate, bilinear form $(\cdot)$, and identify $\hat{Z}$ with Z via the isomorphism $k \in Z \mapsto (k\cdot)$.

We use the letters x, y, or z for points in Z, and the letters k, ℓ for the dual (frequency) variables.

6.2. **Fourier transform.** Denote by $\mathbf{C}^Z$ the complex vector space of functions $Z \to \mathbf{C}$; its dimension if equal to $|Z|$. For $k \in Z$, let $\mathbf{e}_k \in \mathbf{C}^Z$ be the function $x \in Z \mapsto \exp(2i\pi(k \cdot x))$. For the cyclic group $\mathbf{Z}/N\mathbf{Z}$ and the bilinear form described in § 6.1, we obtain $\mathbf{e}_k(x) = \exp(2i\pi kx/N)$.

We endow Z with the equidistributed (or Haar) probability measure $d\nu_Z = \frac{1}{|Z|}\sum_{z\in Z}\delta_z$. The corresponding ℓ^2-norm and scalar product are defined by

$$\| f \|_{\ell^2}^2 = \frac{1}{|Z|}\sum_{z\in Z}|f(z)|^2 \quad \text{and} \quad \langle f|g\rangle = \frac{1}{|Z|}\sum_{z\in Z} f(z)\overline{g(z)} \tag{6.1}$$

for all f, g in $\mathbf{C}^Z$. Then, $(\mathbf{e}_k)_{k\in Z}$ is an orthonormal basis of $\mathbf{C}^Z$ whose elements are characters $Z \to \mathbb{S}^1$. Thus, every function f can be written as $f = \sum_k \hat{f}(k)\mathbf{e}_k$ in a unique way; the Fourier coefficients $\hat{f}(k)$ are given by

$$\hat{f}(k) = \langle f|\mathbf{e}_k\rangle = \frac{1}{|Z|}\sum_{z\in Z} f(z)\overline{\mathbf{e}_k(z)} = \frac{1}{|Z|}\sum_{z\in Z} f(z)\mathbf{e}_{-k}(z). \tag{6.2}$$

The Fourier transform defines a linear map $\mathbf{C}^Z \to \mathbf{C}^Z$, $f \mapsto \hat{f}$, that satisfies

$$\frac{1}{|Z|}\sum_{z\in Z} f(z)\overline{g(z)} = \sum_{k\in Z}\hat{f}(k)\overline{\hat{g}(k)}. \tag{6.3}$$

In other words, it is an isometry for two distinct hermitian products (one does not divide by $|Z|$ on the frequency – or dual – side). Taking $f = g$ one gets Parseval formula

$$\frac{1}{|Z|}\sum_{z\in Z}|f(z)|^2 = \sum_k |\hat{f}(k)|^2. \tag{6.4}$$

Even though the use of the bilinear form $(\,\cdot\,)$ makes it possible to take both the space variable z and the frequency variable k in the same set Z, there is a dissymmetry between them: The frequency k should really be considered as a point $(k\cdot\,)$ in the dual group $\hat{Z}$. The natural measure on frequencies is just $\sum_k \delta_k$, it is not a probability measure. ([3])

[3]This is reflected also in the following remarks. Define $\sigma\colon \mathbf{C}^Z \to C^Z$ by $f^\sigma(z) = f(-z)$ for all $z \in Z$. Then the Fourier transform commutes with σ: $\widehat{f^\sigma} = \left(\hat{f}\right)^\sigma$. Now, if we see $\hat{f}$ as an element of $\mathbf{C}^Z$ and apply the Fourier transform to it, we obtain $\widehat{\hat{f}} = \frac{1}{|Z|}f^\sigma$. But if we see it as an element of $\mathbf{C}^{\hat{Z}}$ and define the Fourier transform on that space by $\hat{g}(x) = \sum_k g(k)\overline{\mathbf{e}_x(k)}$, without division by $|\hat{Z}|$, then $\widehat{\hat{f}} = f^\sigma$.

6.3. **Convolution.** The convolution of f and g is the function $f*g\colon Z\to \mathbf{C}$ defined by

$$f*g(z)=\frac{1}{|Z|}\sum_{x+y=z} f(x)g(y) \tag{6.5}$$

$$=\frac{1}{|Z|}\sum_{x\in Z} f(x)g(z-x). \tag{6.6}$$

(we integrate with respect to the Haar measure on Z). One easily shows that

$$\widehat{f*g}=\hat{f}\cdot\hat{g}. \tag{6.7}$$

6.4. **Equivariance properties.** Let $h\colon Z\to Z$ be an endomorphism of Z. The dual $h^\vee$ of h is the endomorphism of $\hat{Z}$ such that $\xi(h(x))=(h^\vee(\xi))(x)$ for all $(\xi,x)\in\hat{Z}\times Z$; its adjoint h^* is the endomorphism of Z defined by $(h^*(k)\cdot x)=(k\cdot h(x))$ for all $(k,x)\in Z^2$. The isomorphism $Z\to\hat{Z}$, $k\mapsto(k\cdot\ )$, provided by the bilinear form, conjugates h^* to $h^\vee$. With these definitions in mind, one gets

$$\widehat{f\circ h}=\hat{f}\circ h^* \tag{6.8}$$

for every automorphism $h\colon Z\to Z$ and every function $f\in\mathbf{C}^Z$.

Now, consider the translation $t_{z_0}\colon x\in Z\mapsto x+z_0$, for some $z_0\in Z$. Then,

$$\widehat{f\circ t_{z_0}}(k)=\mathbf{e}_k(z_0)\hat{f}(k) \tag{6.9}$$

for all $f\in\mathbf{C}^Z$ and $k\in Z$.

7. Fourier coefficients, following Kurlberg and Rudnick

In this section, following [8]*, we control (some of) the Fourier coefficients of the measures supported on periodic orbits of linear Anosov mapping of the torus* $\mathbf{R}^2/L$.

7.1. **The one dimensional setting.** Fix a positive integer N, and consider the finite cyclic group $Z=\mathbf{Z}/N\mathbf{Z}$. Let H be a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$, the group of invertible elements of $\mathbf{Z}/N\mathbf{Z}$. Then, H acts on Z by multiplication; each orbit Hx has $|H|$ elements except for $x=0$. We set

$$\nu_x=\frac{1}{|H|}\sum_{h\in H}\delta_{hx}; \tag{7.1}$$

this probability measure is evenly distributed on Hx. We also use ν_x to denote the function $Z\to\mathbf{C}$ which is equal to $1/|H|$ on Hx and to 0 on its complement.

By Parseval identity, the Fourier transform of ν_x (in the sense of finite abelian groups) satisfies

$$\frac{1}{|Z|}\frac{1}{|H|} = \sum_{k=0}^{N-1} |\widehat{\nu_x}(k)|^2 \tag{7.2}$$

for every $x \neq 0$. By equivariance, $\widehat{\nu_x}(hk) = \widehat{\nu_x}(k)$ for every $h \in H$. Thus, if we choose a frequency $k_0 \neq 0$ for which $|\widehat{\nu_x}(k_0)| = \max\{|\widehat{\nu_x}(k)|; k \neq 0\}$ we obtain

$$|H||\widehat{\nu_x}(k_0)|^2 \leq (|Z||H|)^{-1}. \tag{7.3}$$

Now, as in § 6.1, consider the homomorphism $\iota\colon Z \to \mathbf{R}/\mathbf{Z}$, $z \mapsto \frac{1}{N}z \mod (\mathbf{Z})$ and the bilinear form $Z \times Z \to \mathbf{R}/\mathbf{Z}$, $(x,y) \mapsto \frac{1}{N}xy \mod (\mathbf{Z})$. Then, $\mu_x := \iota_*\nu_x$ is a probability measure on $\mathbf{R}/\mathbf{Z}$ whose Fourier coefficients

$$\widehat{\mu_x}(k) = \int_0^1 e^{-2i\pi k\theta} d\mu_x(e^{2i\pi\theta}) \tag{7.4}$$

are N-periodic: $\widehat{\mu_x}(k+N) = \widehat{\mu_x}(k)$. Thus, $\widehat{\mu_x}$ can be considered as a function on Z; moreover, $\widehat{\mu_x}(k) = |Z|\widehat{\nu_x}(k)$ for all $k \in Z$. From Equation (7.3) and the definition of k_0, we deduce that

$$|\widehat{\mu_x}(k)| \leq \frac{\sqrt{|Z|}}{|H|} \tag{7.5}$$

for $k \neq 0$. This proves the following result.

Theorem 7.1. *Let $(N_m)_{m\geq 1}$ be an increasing sequence of integers. For each of them, let H_m be a subgroup of $(\mathbf{Z}/N_m\mathbf{Z})^\times$, and let x_m be a non-zero element of $\mathbf{Z}/N_m\mathbf{Z}$. If $N_m = o(|H_m|^2)$, then the sequence of probability measures*

$$\mu_{x_m} = \frac{1}{|H_m|}\sum_{h\in H_m} \delta_{hx_m/N_m}$$

converges to the Haar measure on $\mathbf{R}/\mathbf{Z}$ as m goes to $+\infty$.

7.2. **The 2-dimensional setting.** Consider a positive integer N, set $Z = (\mathbf{Z}/N\mathbf{Z})^2$, and $0 = (0,0)$ the neutral element of Z. Then, embbed Z into $\mathbf{R}^2/\mathbf{Z}^2$ by

$$\iota_N\colon (x_1,x_2) \mapsto (x_1/N, x_2/N) \mod (\mathbf{Z}^2). \tag{7.6}$$

Let H be a subgroup of $\mathsf{GL}_2(\mathbf{Z}/N\mathbf{Z})$. If $x = (x_1,x_2)$ is a point of Z,

$$\nu_x = \frac{1}{|H|}\sum_{h\in H} \delta_{h(x)} = \frac{1}{|H(x)|}\sum_{y\in H(x)} \delta_y \tag{7.7}$$

is a probability measure on Z; it will also be considered as a function, equal to $|H(x)|^{-1}$ on the orbit of x and to 0 on its complement. We set $\mu_x = (\iota_N)_*\nu_x$,

a probability measure on $\mathbf{R}^2/\mathbf{Z}^2$. The Fourier coefficients of μ_x and ν_x are related by

$$\widehat{\mu_x}(k) = |Z|\widehat{\nu_x}(k) = N^2\widehat{\nu_x}(k). \tag{7.8}$$

They satisfy the following relations:

$$\widehat{\nu_x}(h^*(k)) = \widehat{\nu_x}(k) \quad \text{for every} \quad k \in Z, h \in H \tag{7.9}$$

$$\widehat{\nu_{-x}}(k) = \frac{1}{|Z|}\frac{1}{|H|}\sum_{h\in H}\mathbf{e}_k(-h(x)) = \overline{\widehat{\nu_x}(k)}. \tag{7.10}$$

Our goal, now, is to estimate the Fourier coefficients of μ_x and ν_x.

7.3. **Convolutions.** Fix x_0 in Z, and consider the linear operator $P_{x_0}\colon \mathbf{C}^Z \to \mathbf{C}^Z$ defined by

$$P_{x_0}\colon f \mapsto \nu_{x_0} * \nu_{-x_0} * f. \tag{7.11}$$

From Section 6.3 and Equation (7.10), we obtain

$$\widehat{P_{x_0}(f)} = \widehat{\nu_{x_0}}\widehat{\nu_{-x_0}}\hat{f} = |\widehat{\nu_{x_0}}|^2\hat{f}. \tag{7.12}$$

Thus, if $\hat{f}$ is supported on the level set $\{k \in Z\,;\, |\widehat{\nu_{x_0}}(k)|^2 = \lambda\}$, the formula $\widehat{\hat{f}} = |Z|^{-1}f^\sigma$ gives

$$P_{x_0}(f) = \lambda f. \tag{7.13}$$

Since $\widehat{\nu_{x_0}}$ is invariant under the action of H on the space of frequencies, we obtain the following lemma.

Lemma 7.2. *The spectrum of P_{x_0} is the set of values λ of $k \mapsto |\widehat{\nu_{x_0}}(k)|^2$. For such a λ, denote by $V_\lambda \subset \mathbf{C}^Z$ the space of functions $k \mapsto g(k)$ which are supported on $\{k \in Z\,;\, |\widehat{\nu_{x_0}}(k)|^2 = \lambda\}$, and by $W_\lambda \subset \mathbf{C}^Z$ the image of V_λ under the linear map $g \mapsto \hat{g}^\sigma$. Then,*

$$\mathbf{C}^Z = \bigoplus_\lambda W_\lambda,$$

W_λ is the eigenspace of P_{x_0} corresponding to the eigenvalue λ. Moreover,

$$\dim_{\mathbf{C}}(W_\lambda) \geq |H^*(k)|$$

for every k such that $|\widehat{\nu_{x_0}}(k)|^2 = \lambda$.

For $k \geq 1$, $P_{x_0}^k$ corresponds to k successive convolutions with $\nu_{x_0} * \nu_{-x_0}$. The following lemma computes the trace of this operator.

Lemma 7.3. *Set $U_k = \{(p_1,\dots,p_k,q_1,\dots,q_k) \in H(x_0)^{2k}\,;\, \sum_i p_i = \sum_i q_i\}$. Then, the trace of $P_{x_0}^k$ is given by*

$$\mathsf{Tr}(P_{x_0}^k) = \frac{|U_k|}{|Z|^{2k-1}|H(x_0)|^{2k}}.$$

Proof. Consider the orthonormal basis of $\mathbf{C}^Z$ defined by the functions $|Z|^{1/2}\delta_x$, for x in Z. The scalar product $\langle P_{x_0}^k(|Z|^{1/2}\delta_x) \mid |Z|^{1/2}\delta_x\rangle$ is equal to

$$|Z|\langle P_{x_0}^k(\delta_x) \mid \delta_x\rangle = \sum_{y\in Z}(P_{x_0}^k(\delta_x))(y)\delta_x(y) = (P_{x_0}^k(\delta_x))(x); \tag{7.14}$$

since $P_{x_0}^k$ corresponds to k successive convolutions with $\nu_{x_0} * \nu_{-x_0}$, we obtain

$$= \frac{1}{|Z|^{2k}}\frac{1}{|H(x_0)|^{2k}} \sum_{p_1,\dots,p_k,q_1,\dots,q_k} \delta_x(x+\sum_i p_i - \sum_i q_i) \tag{7.15}$$

$$= \frac{|U_k|}{(|Z|\cdot|H(x_0)|)^{2k}} \tag{7.16}$$

where the p_i and q_j in the sum are elements of $H(x_0)$. The result follows by summation over x. □

7.4. **Kurlberg-Rudnick upper bounds: Prime moduli.** We follow first the argument of [8] in the simplest case, namely when N is a prime p. Let B be an element of $\mathsf{SL}_2(\mathbf{F}_p)$. We denote by $\Delta_B = \mathsf{Tr}(B)^2 - 4$ the discriminant of the characteristic polynomial of B and we assume that p does not divide Δ_B. In this case, the eigenvalues α, $1/\alpha$ of B live in $\mathbf{F}_p$ (resp. $\mathbf{F}_{p^2}$) if Δ_B is a square modulo p (resp. is not a square modulo p). In both cases, $\alpha \neq \alpha^{-1}$ since $\Delta_B \neq 0 \mod (p)$; in particular, B is diagonalisable over $\mathbf{F}_{p^2}$.

Lemma 7.4. *Assume $\Delta_B \neq 0 \mod (p)$. If $x \in \mathbf{F}_p^2 \setminus \{0\}$ is not an eigenvector of B, then*

$$\forall M \in \mathbf{F}_p[B],\ (Mx = 0) \Leftrightarrow (M = 0).$$

Moreover $x \in \mathbf{F}_p^2 \setminus \{0\}$ is not an eigenvector if Δ_B is not a square $\mod (p)$.

Proof. Fix $x \in \mathbf{F}_p^2 \setminus \{0\}$. By Cayley-Hamilton theorem, we can write $M = aB + b\mathsf{Id}$ for some pair $(a,b) \in \mathbf{F}_p^2$. Now, $Mx = 0$ if and only if $aBx = -bx$, if and only if x is an eigenvector of B or $(a,b) = 0$. □

As above, set $Z = \mathbf{F}_p \times \mathbf{F}_p$, and let H be the subgroup of $\mathsf{SL}_2(\mathbf{F}_p)$ generated by B. All nonzero orbits of H (or H^*) on Z have $|H|$ elements: Indeed, the order of B is the mutiplicative order of α which is the same as the order of α^{-1}.

Lemma 7.5 (Kurlberg-Rudnick, see Lemma 5 of [8])**.** *The equation $h_1 + h_2 = h_3 + h_4$ in H^4 has*

- *$|H|^2$ solutions (h_1,h_2,h_3,h_4) for which $h_1 + h_2 = 0$;*
- *$2|H|^2 - |H|$ solutions (h_1,h_2,h_3,h_4) for which $h_1 + h_2 \neq 0$; for such a solution, we have $\{h_1,h_2\} = \{h_3,h_4\}$.*

Altogether, there are less than $3|H|^2$ *solutions.*

Proof. In the case of the first item, we have $h_2 = -h_1$, $h_4 = -h_3$, where (h_1, h_3) is any element of $H \times H$. For the second case, write B in diagonal form over $\overline{\mathbf{F}_p}$, and denote by x_i and x_i^{-1} the eigenvalues of h_i. We obtain $x_1 + x_2 = x_3 + x_4$ and $x_1^{-1} + x_2^{-1} = x_3^{-1} + x_4^{-1}$. The second equality implies $(x_1 + x_2)/(x_1x_2) = (x_3 + x_4)/(x_3x_4)$ so $x_1x_2 = x_3x_4$. In particular, $\{x_1, x_2\}$ and $\{x_3, x_4\}$ have the same sum and product: Both couples are the two solutions of the same quadratic equation, so $\{x_1, x_2\} = \{x_3, x_4\}$. This shows that $\{h_1, h_2\} = \{h_3, h_4\}$ and gives $2|H|^2 - |H|$ new solutions, namely $2(|H|^2 - |H|)$ choices where h_1, h_2 are distinct, and $|H|$ choices where $h_1 = h_2 = h_3 = h_4$. □

Corollary 7.6 (Kurlberg-Rudnick)**.** *Assume that* $\Delta_B \neq 0 \mod (p)$ *and* $x_0 \in Z \setminus \{0\}$ *is not an eigenvector of B. Then* $|U_2| \leq 3|H|^2$ *and*

$$\mathsf{Tr}(P_{x_0}^2) \leq \frac{3}{|Z|^3|H|^2}.$$

Proof. Consider the equation $h_1(x_0) + h_2(x_0) = h_3(x_0) + h_4(x_0)$. By Lemma 7.4, it is equivalent to the one solved in the previous lemma. Thus, we have at most $3|H|^2$ solutions. The conclusion follows from Lemma 7.3. □

Now, under the above assumptions, for every $k \in Z$, Lemma 7.2 gives

$$|\widehat{\nu_{x_0}}(k)|^4 \leq \frac{3}{|Z|^3|H|^2} \frac{1}{|H^*(k)|}. \tag{7.17}$$

If $k \neq 0$, our assumptions imply $|H^*(k)| = |H|$ and from $|\widehat{\mu_{x_0}}(k)| = |Z||\widehat{\nu_{x_0}}(k)|$ we derive

$$|\widehat{\mu_{x_0}}(k)|^4 \leq 3\frac{p^2}{|H|^3} \qquad (\forall k \neq 0)$$

because $|Z| = p^2$. This would be sufficient to show that the Fourier coefficients were small if we knew that $|H| \gg p^{2/3}$, but the Corollary 4.5 only gives at best an exponent $3/5 < 2/3$. Our next result improves upon this type of inequality down to the exponent $1/2$.

Theorem 7.7. *Let B be an element of* $\mathsf{SL}_2(\mathbf{F}_p)$ *with* $\Delta_B \neq 0 \mod (p)$ *and let* $H \subset \mathsf{SL}_2(\mathbf{F}_p)$ *be the group generated by B. Let* x_0*, k be non-zero elements of* $\mathbf{F}_p^2$*. If* x_0 *is not an eigenvector for B and k is not an eigenvector for* B^**, then the k-th Fourier coefficient of* μ_{x_0} *satisfies*

$$|\widehat{\mu_{x_0}}(k)|^4 \leq 2\sqrt{3}\frac{p}{|H|^2}.$$

Example 7.8. For $p = 1973$, the order of A is 1316 and the order of $B = A^2$ is 658. Then $2\sqrt{3}p|H|^{-2} \simeq 0.016$.

Proof. We start with the following computation, in which $Z = \mathbf{F}_p \times \mathbf{F}_p$,

$$\begin{aligned}
|Z|^2|\widehat{\nu_{x_0}}(k)|^2 &= \frac{1}{|H|^2}\sum_{g\in H}\sum_{g'\in H}\mathbf{e}_{-k}(g(x_0))\mathbf{e}_k(g'(x_0)) \\
&= \frac{1}{|H|^2}\sum_{g\in H}\sum_{g'\in H}\mathbf{e}_{-g^*k}(x_0)\mathbf{e}_{g^*k}(g^{-1}g'(x_0)) \\
&= \frac{1}{|H|^2}\sum_{g\in H}\sum_{h\in H}\mathbf{e}_{g^*k}(-x_0)\mathbf{e}_{g^*k}(h(x_0)) \\
&= \frac{1}{|H|^2}\sum_{g\in H}\sum_{h\in H}\mathbf{e}_{g^*k}((h-\mathsf{Id})(x_0)) \\
&= \frac{1}{|H|}\sum_{h\in H}\frac{1}{|H|}\sum_{g\in H}\mathbf{e}_{(h-\mathsf{Id})^*k}(g(x_0)) \\
&= \frac{1}{|H|}\sum_{h\in H}|Z|\widehat{\nu_{x_0}}((h^*-\mathsf{Id})(k)).
\end{aligned}$$

(The third equality is obtained by re-indexing the sum by setting $h = g^{-1}g'$ and the fifth equality uses that $(h-\mathsf{Id})$ and g commute for all g, h in H.) Now, we apply the Hölder inequality with weights $4/3$ and 4; this gives

$$\begin{aligned}
|\widehat{\mu_{x_0}}(k)|^2 &\le \frac{|Z|}{|H|}\left(\sum_{h\in H}1\right)^{3/4}\left(\sum_{h\in H}|\widehat{\nu_{x_0}}((h^*-\mathsf{Id})(k))|^4\right)^{1/4} \\
&\le \frac{|Z|}{|H|^{1/4}}\left(\sum_{h\in H}|\widehat{\nu_{x_0}}((h^*-\mathsf{Id})(k))|^4\right)^{1/4} \qquad (7.18)
\end{aligned}$$

Lemma 7.9. *For $k \in Z\setminus\{0\}$ which is not an eigenvector of B^*, the set $\{(h^*-\mathsf{Id})(k)\ ;\ h\in H\}$ intersects any H^*-orbit in at most two points.*

Proof of the lemma. Assume $h_1(k)-k = h_3(h_2(k)-k)$ for some triple of elements of H^* with $h_1 \neq h_2$. We will show that the only possibility is $h_2 = h_1^{-1}$. By Lemma 7.4, we obtain $h_1+h_3 = h_3h_2+\mathsf{Id}$, and according to Lemma 7.5 only two cases may occur. Either $h_1+h_3 = 0$ and $h_3h_2+\mathsf{Id} = 0$, so $h_2 = h_1^{-1}$. Or $h_1+h_3 \neq 0$, but then $\{h_1,h_3\} = \{h_3h_2,\mathsf{Id}\}$ in contradiction with $h_1 \neq h_2$. □

Thus, if we partition the frequency plane $Z = \mathbf{F}_p^2$ into H^*-orbits, and if we remember that each H^*-orbit has $|H|$ elements except for $H(0)$, we obtain

$$\begin{aligned}|\widehat{\mu_{x_0}}(k)|^2 &\leq \frac{|Z|}{|H|^{1/4}}\left(|\widehat{\nu_{x_0}}(0)|^4 + \sum_{h\in H, h\neq \mathsf{Id}} |\widehat{\nu_{x_0}}((h^*-\mathsf{Id})(k))|^4\right)^{1/4}\\ &\leq \frac{|Z|}{|H|^{1/4}}\left(\frac{1}{|Z|^4} + \frac{2}{|H|}\sum_{\ell\in Z,\ell\neq 0}|\widehat{\nu_{x_0}}(\ell)|^4\right)^{1/4}\\ &\leq \frac{|Z|}{|H|^{1/4}}\left(\frac{1}{|Z|^4} + \frac{2}{|H|}\mathsf{Tr}(P_{x_0}^2)\right)^{1/4}.\end{aligned}$$

If $\mathsf{Tr}(P_{x_0}^2) \geq \frac{|H|}{2|Z|^4}$ we obtain

$$|\widehat{\mu_{x_0}}(k)|^2 \leq \frac{|Z|}{|H|^{1/4}}\left(\frac{4}{|H|}\mathsf{Tr}(P_{x_0}^2)\right)^{1/4}.$$

Thus, by Corollary 7.6, we conclude that

$$|\widehat{\mu_{x_0}}(k)|^2 \leq \left(12\frac{|Z|}{|H|^4}\right)^{1/4} = \left(12\frac{p^2}{|H|^4}\right)^{1/4}.$$

And if the opposite inequality $\mathsf{Tr}(P_{x_0}^2) \leq \frac{|H|}{2|Z|^4}$ is satisfied, we already knew that $|\widehat{\nu_{x_0}}(k)|^2 \leq 2|Z|^{-4}$ for all non-zero frequency. □

7.5. **Kurlberg-Rudnick upper bounds: Composite moduli.** While necessary for Theorem C, this section may be skipped in a first reading: For instance, Section 8.2 how Theorem D can be derived directly from Theorem 7.7.

We now consider a matrix $B \in \mathsf{SL}_2(\mathbb{Z})$, with discriminant $\Delta_B = \mathsf{Tr}(B)^2 - 4 \neq 0$. Let N be a positive integer and set $Z = (\mathbf{Z}/N\mathbf{Z})^2$. Let x_0 and k be non-zero elements of Z. Let H be the subgroup of $\mathsf{SL}_2(\mathbf{Z}/N\mathbf{Z})$ generated by the class of B modulo N. For any divisor d of N, we denote with an index d the image of any object by the induced morphism $\mathbf{Z}/N\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$; for example H_d is the group generated by the class B_d of B in $\mathsf{SL}_2(\mathbf{Z}/d\mathbf{Z})$.

Our goal is to extend the inequalites of the previous section to the setting of arbitrary moduli N instead of prime moduli. For this, we consider a parameter $D > 0$ and assume that N can be written

$$N = Mq, \tag{7.19}$$

where, roughly speaking, the number M will act as a bounded "dump" where we threw all the factors we don't want to hear about, and will be much smaller than q. More precisely, we shall assume that

(Ω1).– M and q are coprime integers,
(Ω2).– q is squarefree and $q = \prod_{p\in I} p$ for a set I of primes $p \geq D$,
(Ω3).– $\Delta_B < D$, hence for all $p \in I$, $\Delta_B \neq 0 \mod (p)$,
(Ω4).– for all $p \in I$, $(x_0)_p$ is nonzero and not an eigenvector for B_p, and k_p is nonzero and not an eigenvector for B_p^*.

This set of hypotheses on B, N, M, D, q, x_0, k will be denoted by (Ω). We denote by $\omega = |I|$ the number of prime factors of q. Similarly to [8, Lemma 7], we first note

Lemma 7.10. *Under the hypotheses (Ω), we have the following properties.*

(1) $|H_q| \leq |H| \leq M^3 |H_q|$.
(2) *If $x \in Z$ is nonzero modulo every $p \in I$, then $|H(x)| \geq |H|/M^3$.*
(3) *The equation $h_1 + h_2 = h_3 + h_4$ in H_q^4 has at most $3^\omega |H_q|^2$ solutions.*
(4) *The trace of $P_{x_0}^2$ satisfies*

$$\mathsf{Tr}(P_{x_0}^2) \leq \frac{3^\omega M^{24}}{|Z|^3 |H|^2}.$$

Proof. Since M and q are coprime, the map $H \to H_M \times H_q$, $h \mapsto (h_M, h_q)$ is injective. Therefore the kernel of the surjective homomorphism $H \to H_q$, $h \mapsto h_q$ is at most of size $|H_M| \leq |\mathsf{SL}_2(\mathbf{Z}/M\mathbf{Z})| \leq M^3$. This proves (1).

Let us check (2). Let $h \in H$ be in the stabiliser of x. By assumption, the image x_p of x modulo p is nonzero for every $p \in I$; so $h_p(x_p) = x_p$ implies $h_p = \mathsf{Id}$ for all $p \in I$, and $h_q = \mathsf{Id}$. Therefore the stabiliser of x in H is in the kernel of $h \mapsto h_q$ which is of cardinality bounded by M^3.

For (3), observe that for every prime p, $|H_p| = \mathrm{ord}_B(p)$ is the order of B modulo p; thus, $|H_q|$ is the least common multiple of the $|H_p|$, $p \in I$. In particular, if we decompose $|H_q| = u_1^{\alpha_1} \cdots u_r^{\alpha_r}$ as a product of distinct prime powers, then for any $i = 1, \ldots, r$ we can choose a $p(i) \in I$ such that $u_i^{\alpha_i}$ divides $|H_{p(i)}|$. By grouping the $u_i^{\alpha_i}$ according to the value of $p(i)$, we obtain

$$|H_q| = \prod_{p\in I} n_p \quad \text{with} \quad n_p = \prod_{j : p(j) = p} u_j^{\alpha_j}; \tag{7.20}$$

the n_p are coprime to each other, and n_p divides $|H_p|$. By Lemma 7.5, if (a, b, c, d) is a solution to the equation

$$B^a + B^b = B^c + B^d \mod (p), \tag{7.21}$$

for some $p \in I$, then

- either $B^a + B^b = 0 \mod (p)$, so $a = b + t_p \mod (|H_p|)$ and $c = d + t_p \mod (|H_p|)$ where t_p is an exponent such that $B^{t_p} = -\mathsf{Id} \mod (p)$,
- or $\{a,b\} = \{c,d\} \mod (|H_p|)$.

These congruences for the exponents are still true modulo n_p; this gives at most $3n_p^2$ possibilities for (a,b,c,d) modulo n_p. Since the n_p are coprime to each other, the Chinese remainder theorem shows that there are at most $3^{|I|}\prod_p n_p^2 = 3^\omega |H_q|^2$ solutions to the equation $B^a + B^b = B^c + B^d \mod (q)$.

Now, assertion (4) is shown in the same way as Corollary 7.6. By Lemma 7.3, we have

$$\mathsf{Tr}(P_{x_0}^2) = \frac{|U_2|}{|Z|^3 |H(x_0)|^4}, \tag{7.22}$$

where $|U_2|$ is the number of solutions modulo N to

$$h_1(x_0) + h_2(x_0) = h_3(x_0) + h_4(x_0). \tag{7.23}$$

Consider this equation modulo p, for $p \in I$. By (Ω4), $(x_0)_p$ is not an eigenvector of B_p, so Lemma 7.4 applies and we get

$$h_1 + h_2 = h_3 + h_4 \mod (p); \tag{7.24}$$

by the Chinese remainder theorem, this equation is still satisfied in H_q. This gives at most $3^\omega |H_q|^2$ possibilities for (h_1,h_2,h_3,h_4) modulo q, hence at most $M^{12} 3^\omega |H_q|^2$ possibilities modulo N. Since $|H(x_0)| \geq |H|/M^3$, we get the desired upper bound. □

To control the size of the Fourier coefficients of μ_{x_0}, we shall use the following notations:

$$\kappa = \inf_{p \in I} \mathrm{ord}_B(p) = \inf_{p \in I} |H_p|, \tag{7.25}$$

and

$$\check{H} = \{h \in H : \forall p \in I, h_p \neq \mathsf{Id}\}. \tag{7.26}$$

The complement $H \setminus \check{H}$ is the union of ω subgroups of index at least κ, so

$$|H - \check{H}| \leq \omega \frac{|H|}{\kappa}. \tag{7.27}$$

Here is the analogue of Lemma 7.9:

Lemma 7.11. *Under the hypotheses* (Ω), *the family* $\{(h^* - \mathsf{Id})(k) \,;\, h \in \check{H}\}$

(1) *intersects each H^*-orbit in at most $2^\omega M^3$ points (counted with multiplicities, since it may happen that $h \mapsto (h^* - \mathsf{Id})(k)$ is not injective),*
(2) *does not intersect any H^*-orbits of cardinality $\leq |H|/M^3$.*

Proof. Given $h_1 \in H^*$, the equation

$$(h_1 - \mathsf{Id})(k) = h_3(h_2 - \mathsf{Id})(k), \tag{7.28}$$

in the variables $h_2, h_3 \in H^*$ can be reduced modulo p for $p \in I$. By (Ω4) k_p is nonzero nor an eigenvector of B_p^*; thus, by (Ω3), we can apply Lemma 7.4 and we obtain

$$(h_1 - \mathsf{Id}) = h_3(h_2 - \mathsf{Id}) \mod (p); \tag{7.29}$$

then, as in the proof of Lemma 7.9, the only solutions are $(h_2)_p = (h_1)_p^{\pm 1}$. Thus given h_1, there are only 2^ω possibilities for $(h_2)_q \in H_q$, hence at most $2^\omega M^3$ possibilities for $h_2 \in H$ (see Lemma 7.10(1)).

Let us now check the second claim. If $h \in \check{H}$, then for all $p \in I$, we can apply again (Ω3), (Ω4), and Lemma 7.4 to get $h_p^* k_p \neq k_p$. So the vector $(h^* - \mathsf{Id})(k)$ satisfies the assumption of Lemma 7.10, and Lemma 7.10(2) gives the result. □

Theorem 7.12. *Under the set of assumptions* (Ω)*, we have*

$$|\widehat{\mu_{x_0}}(k)|^4 \leq \sqrt{\frac{\omega}{\kappa}} + \frac{6^{\omega/2} M^{15} N}{|H|^2}.$$

Proof. Equation (7.18) (and its proof) is still valid for the composite moduli N,

$$|\widehat{\mu_{x_0}}(k)|^2 \leq \frac{|Z|}{|H|^{1/4}} \left(\sum_{h \in H} |\widehat{\nu_{x_0}}((h^* - \mathsf{Id})(k))|^4 \right)^{1/4}; \tag{7.30}$$

cutting the sum in two, and using the trivial bound $|\widehat{\nu_{x_0}}| \leq 1/|Z|$, we get

$$|\widehat{\mu_{x_0}}(k)|^2 \leq \frac{|Z|}{|H|^{1/4}} \left(\sum_{h \in H - \check{H}} \frac{1}{|Z|^4} + \sum_{h \in \check{H}} |\widehat{\nu_{x_0}}((h^* - \mathsf{Id})(k))|^4 \right)^{1/4}. \tag{7.31}$$

By the bound (7.27), H^*-invariance of $\widehat{\nu_{x_0}}$ and Lemma 7.11,

$$|\widehat{\mu_{x_0}}(k)|^4 \leq \frac{|Z|^2}{|H|^{1/2}} \left(\frac{\omega |H|}{\kappa |Z|^4} + \frac{2^\omega M^6}{|H|} \sum_{\ell \in Z} |\widehat{\nu_{x_0}}(\ell)|^4 \right)^{1/2}, \tag{7.32}$$

and since $\sqrt{a+b} \leq \sqrt{a} + \sqrt{b}$ for all positive a, b, Lemma 7.2 gives

$$|\widehat{\mu_{x_0}}(k)|^4 \leq \frac{\omega^{1/2}}{\kappa^{1/2}} + \frac{2^{\omega/2} M^3 |Z|^2}{|H|} \mathsf{Tr}(P_{x_0}^2)^{1/2}, \tag{7.33}$$

Using now Lemma 7.10 (4), we obtain

$$|\widehat{\mu_{x_0}}(k)|^4 \leq \frac{\omega^{1/2}}{\kappa^{1/2}} + \frac{6^{\omega/2} M^{15} |Z|^{1/2}}{|H|^2}, \tag{7.34}$$

as required. □

8. When the Farfalle disappears: Equidistribution

We collect all previous results to prove Theorems C and D. To warm up, we start with a remark on the distribution of "random" periodic orbits.

8.1. **Random periodic orbits.** Say that a probability measure μ on $\mathbf{R}^2/L$ is **ε-well distributed** if its Fourier coefficients satisfy $\hat{\mu}(k) < \varepsilon$ for every $k \neq 0$ such that $\| k \| < 1/\varepsilon$. A sequence of probability measures (μ_n) on $\mathbf{R}^2/L$ converges towards the Haar measure of the torus if and only if, for every $\varepsilon > 0$, μ_n becomes ε-well distributed as n goes to ∞. Similarly, a non-empty, finite set $S \subset \mathbf{R}^2/L$ is ε-well distributed if so is the average measure

$$\mu_S := \frac{1}{|S|} \sum_{s \in S} \delta_s.$$

We shall apply these definitions for the empirical measures μ_S, when S is the A-orbit of a point $\iota_N(x)$, for $x \in (\mathbf{Z}/N\mathbf{Z})^2$ (see the notation of Section 7.2); equivalently, S is the A-orbit of a point in $(\frac{1}{N}\mathbf{Z}^2)/L$.

Theorem 8.1. *Given any positive ε, the proportion of points in $(\frac{1}{N}\mathbf{Z}^2)/L$ with an ε-well distributed A-orbit converges towards 1 as N goes to $+\infty$.*

Thus, for N large, if we pick a point x at random among all periodic points in $(\frac{1}{N}\mathbf{Z}^2)/L$ then, with a high probability, the measure μ_x is well distributed.

Proof. We identify $(\frac{1}{N}\mathbf{Z}^2)/L$ with $(\mathbf{Z}/N\mathbf{Z})^2$ via the homomorphism ι_N. If x is an element of $(\mathbf{Z}/N\mathbf{Z})^2$ (resp. of $\mathbf{Z}^2$), we denote by $\mathrm{per}_x(N)$ its period under the action of A (resp. its period modulo N). Fix a frequency $k = (k_1, k_2)$ in $\mathbf{Z}^2 \setminus \{0\}$ and set

$$\mathrm{Bad}_N(k) = \{x \in (\mathbf{Z}/N\mathbf{Z})^2; |\widehat{\mu_x}(k)| \geq \varepsilon\}. \tag{8.1}$$

Since A is symmetric, $\widehat{\mu_x}(k) = \widehat{\mu_k}(x)$; thus, by Parseval formula (see Equation (6.4) and the relation $\widehat{\mu_x}(k) = N^2 \widehat{\nu_x}(k)$ from Equation (7.8)), we get

$$\sum_x |\widehat{\mu_x}(k)|^2 = \sum_x |\widehat{\mu_k}(x)|^2 = \frac{1}{N^2} \sum_\ell |\mu_k(\ell)|^2 = \frac{N^2}{\mathrm{per}_k(N)}. \tag{8.2}$$

The period of k modulo N satisfies $\mathrm{per}_k(N) \geq \log(N \parallel k \parallel_\infty^{-1})$, where $\parallel k \parallel_\infty = \max(|k_1|, |k_2|)$. Indeed, the integral vector $A^m(k) - k$ is non-zero in $\mathbf{Z}^2$, and its norm satisfies $\parallel A^m(k) - k \parallel_\infty \leq \parallel A \parallel_\infty^{m+1} \parallel k \parallel_\infty$; thus, to get $A^m k = k \mod (N)$, we must have $(m+1)\log(\parallel A \parallel_\infty) \geq \log(N \parallel k \parallel_\infty^{-1})$, which gives the result because $\parallel A \parallel_\infty = 2$. Altogether, we obtain the following upper bound on the proportion of bad points:

$$\frac{|\mathrm{Bad}_N(k)|}{N^2} \leq \frac{1}{\varepsilon^2 \log(N \parallel k \parallel_\infty^{-1})}. \tag{8.3}$$

Considering only frequencies $k \neq 0$ in $\mathbf{Z}^2$ with $\parallel k \parallel_\infty < 1/\varepsilon$, we get

$$\frac{|\mathrm{Bad}_N(k)|}{N^2} \leq \frac{1}{\varepsilon^2 \log(N\varepsilon)}. \tag{8.4}$$

Since there are at most $(2\varepsilon^{-1}+1)^2$ integer points in $\mathbf{Z}^2$ with ℓ^∞-norm $< 1/\varepsilon$, the proportion of starting points x for which μ_x has a Fourier coefficient $> \varepsilon$ for some frequency $k \neq 0$ of norm $< 1/\varepsilon$ is at most $(2\varepsilon^{-1}+1)^2 \varepsilon^{-2} (\log(N\varepsilon))^{-1}$. Since ε is fixed, this proportion goes to 0 as N goes to $+\infty$. □

8.2. **Prime moduli: Proof of Theorem D.** In this section, we shall prove the following results, the first two being stronger forms of Theorem D. Recall that Chebotarev's density Theorem implies that the relative density of primes congruent to $1, 4 \mod (5)$ is $1/2$, and the same holds for $p \equiv 2, 3 \mod (5)$.

Theorem 8.2. *There is a set K_1 of prime numbers such that*

(a) *$p = 1$ or $4 \mod (5)$ for every $p \in K_1$;*
(b) *the relative density of K_1 among all primes is positive;*
(c) *if p_k is an increasing sequence of elements of K_1, then the sequence of measures (μ_{p_k}) converges towards the Haar measure on $\mathbf{R}^2/L$.*

Theorem 8.3. *There is a set K_2 of prime numbers such that*

(a) *$p = 2$ or $3 \mod (5)$ for every $p \in K_2$;*
(b) *the relative density of K_2 among all primes is equal to $1/2$;*
(c) *if p_k is an increasing sequence of elements of K_2, then the sequence of measures (μ_{p_k}) converges towards the Haar measure on $\mathbf{R}^2/L$.*

Theorem 8.4. *Assuming GRH, there is a set K_3 of prime numbers of full relative density among all primes, such that if p_k is an increasing sequence of elements of K_3, then the sequence of measures (μ_{p_k}) converges towards the Haar measure on $\mathbf{R}^2/L$.*

8.2.1. *Prime moduli, large order and equidistribution.* Theorems 8.2 and 8.4 will be derived from the following statement.

Proposition 8.5. *If (p_ℓ) is an increasing sequence of primes such that*

$$\lim_{\ell\to+\infty} \frac{\sqrt{p_\ell}}{\mathrm{ord}_A(p_\ell)} = 0$$

then (μ_{p_ℓ}) converges towards the Haar measure on $\mathbf{R}^2/L$

Proof. Set $B = A^2 \in \mathsf{SL}_2(\mathbf{Z})$ and $B_\ell = A^2 \mod (p_\ell)$; let H_ℓ be the subgroup of $\mathsf{SL}_2(\mathbf{F}_{p_\ell})$ generated by B_ℓ. These B_ℓ satisfy the starting assumptions of Section 7.4. Define $x_\ell = (0,1) \in \mathbf{F}_{p_\ell}^2$; this point is mapped to the point $P_\ell = (0,1/p_\ell)$ under the homomorphism ι_{p_ℓ} that maps $(a,b) \in \mathbf{F}_{p_\ell}^2$ to $(a/p_\ell, b/p_\ell) \in \mathbf{R}^2/L$. Notice that the measure

$$\mu_p = \frac{1}{\mathrm{per}_A(P_p)} \sum_{n=1}^{\mathrm{per}_A(P_p)} \delta_{f_A^n(P_p)}$$

can be written as the average of the atomic measure equidistributed on the f_B-orbit of $\iota_{p_\ell}(x_\ell)$, and the atomic measure equidistributed on the f_B-orbit of $\iota_p(A(x))$, with $A(x) = (1,1)$. It is thus sufficient to prove the same statement for B and any fixed, non-zero initial point $x_0 \in \mathbf{Z}^2$.

We thus fix such an x_0, and denote by $\mu_{x_0,\ell}$ the atomic measure on the f_B-orbit of $\iota_{p_\ell}(x_0)$. Fix a frequency $k \neq 0$ in $\mathbf{Z}^2$, and remark that:

Lemma 8.6. *There exists $D > 0$, that depends on $x_0 \neq 0$, such that for all primes $p > D$, $(x_0)_p$ is nonzero and not an eigenvector of B_p.*

Proof. Recall that Δ_B denotes the discriminant, here equal to 5 since $B = A^2$. Fix an equation $ax + by = 0$ of one of the eigenlines of B with (a,b) in $\mathbf{Z}(|\Delta_B|^{1/2})$; the second eigenline is determined by the equation $a'x + b'y = 0$, where a' and b' are the Galois conjugates of a and b; the product $Q(x,y) = (ax+by)(a'x+b'y)$ is a B-invariant quadratic form and is defined over $\mathbf{Z}$. By assumption, $Q(x_0)$ is a non-zero integer. If $p > \max(|\det(Q)|, |\Delta_B|)$, then Q_p is non-degenerate and its isotropic cone (computed in $\overline{\mathbf{F}_p} \times \overline{\mathbf{F}_p}$) is the union of the two eigenlines of B_p. Now, if p is larger than the maximum of $|\det(Q)|$, $|\Delta_B|$, and $|Q(x_0)|$, then $(x_0)_p$ is non-zero, and is not an eigenvector of B_p. □

According to Lemma 8.6, if ℓ is large enough, then the reduction of k and of x_0 modulo p_ℓ are non-zero and are not eigenvectors of B^* or B. Thus, we can apply Theorem 7.7. The order of B_ℓ in $\mathsf{SL}_2(\mathbf{F}_{p_\ell})$ being at least $\mathrm{ord}_A(p_\ell)/2$, the Fourier coefficient $\widehat{\mu}_{x_0,\ell}(k)$ converges towards 0 as ℓ goes to $+\infty$.

Now, by Weyl's criterium, $\mu_{x_0,\ell}$ converges towards the Haar measure, as required. □

8.2.2. *The case* $p \equiv 1,4 \mod (5)$. Here we prove Theorem 8.2. Fix some ε in $]0, \frac{1}{10}[$. According to Corollary 4.5 there is a set K_1 of prime numbers, such that K_1 has positive relative density and the elements p of K_1 satisfy $p = 1,4 \mod (5)$ and $\mathrm{ord}_A(p) \geq p^{\frac{3}{5}-\varepsilon}$. Thus, Proposition 8.5 applies.

8.2.3. *Assuming GRH.* Fix $\varepsilon > 0$ small. If we assume the Generalized Riemann Hypothesis, the result of Kurlberg described in Remark 4.6 provides a set K_3 of full density among the primes, such that $\mathrm{ord}_B(p) > p^{1-\varepsilon}$ for all $p \in K_3$. This and Proposition 8.5 prove Theorem 8.4.

8.2.4. *The case* $p \equiv 2,3 \mod (5)$. In this case we do not use the estimate on the Fourier coefficients given by Theorem 7.7, but a Theorem of Bourgain and Glibichuk [1].

Proof of Theorem 8.3. Fix $\alpha = 1/2 - \eta$ for some small η, and consider the set K_2 of primes p such that (a) $p = 2$ or $3 \mod (5)$ and (b) $\mathrm{ord}_A(p) \geq p^{\alpha}$. By Chebotarev's theorem and Lemma 4.3, this set has density $1/2$ among all primes. Fix p in K_2 and consider the Fibonacci matrix A modulo p. By definition of K_2, its order in $\mathsf{GL}_2(\mathbf{F}_p)$ is $\geq p^{\alpha}$. Moreover, since 5 is not a square modulo p, the eigenvalues φ and φ' of A live in a quadratic extension $\mathbf{F}$ of $\mathbf{F}_p$. As an $\mathbf{F}_p$-vector space, $\mathbf{F}_p \times \mathbf{F}_p$ can be identified to $\mathbf{F}$ by the linear isomorphism $(a,b) \mapsto a + b\varphi$: This conjugates the linear action of A on $\mathbf{F}_p \times \mathbf{F}_p$ to the multiplication by φ on $\mathbf{F}$.

Denote the trace by $Tr\colon \mathbf{F} \to \mathbf{F}_p$. By definition, $Tr(a+b\varphi) = 2a + b(\varphi + \varphi') = 2a - b$, or equivalently $Tr(x) = x + x^p$, since $x \mapsto x^p$ is the Galois automorphism. Every linear map $\mathbf{F} \to \mathbf{F}_p$ can be written as $x \mapsto Tr(\xi x)$ for some $\xi \in \mathbf{F}$. With this notation at hand, Theorem 5 of [1] says precisely that, for any non-zero frequencies $k = (k_1, k_2)$, the Fourier coefficients $\widehat{\mu_p}(k)$ converge towards 0 as $p \in K_2$ goes to ∞. Indeed, this theorem can be applied to the cyclic group H generated by φ in $\mathbf{F}_q^{\times}$; the hypothesis $|H \cap \mathbf{F}_p| < |H|^{1-\eta}$ is satisfied for the following reason. Since the Galois conjugate φ' of φ is $-\varphi^{-1}$, the conjugate of any element $x \in H$ is equal to $\pm x^{-1}$; thus the elements of $H \cap \mathbf{F}_p$ are fourth roots of unity, so in fact $|H \cap \mathbf{F}_p| \leq 4$. This proves the theorem. □

8.3. **Proof of Theorem C.** The goal is to show that along a set $K \subset \mathbf{N}$ of density 1, the measures $(\mu_N)_{N \in K}$ converge toward the Haar measure. Like in the proof of Theorem 8.2, we set $B = A^2$ and we fix a non-zero initial point

$x_0 \in \mathbf{Z}^2$; we denote by $\mu_{x_0,N}$ the atomic measure on the orbit of $\iota_N(x_0)$ and by H_N the subgroup of $\mathsf{SL}_2(\mathbf{Z}/N\mathbf{Z})$ generated by B modulo N.

8.3.1. *Step 1.* We prove the following: *Given* $\eta \in]0,1[$ *and* $k \in \mathbf{Z}^2 \setminus \{0\}$*, the set*

$$X_{\eta,k} = \{N > 0;\ |\widehat{\mu_{x_0,N}}(k)|^4 \leq \eta\},$$

is a subset of $\mathbf{N}$ *of density* 1.

We fix $k \neq 0$. There exists an integer D_k such that Lemma 8.6 holds for both (B, x_0) and (B^*, k). By the fourth assertion in Section 4.2, we obtain:

Lemma 8.7. *There exists a constant* $C > 0$*, such that*

$$ord_B(p) = |H_p| \geq C\log(p)$$

for every prime p*; one can take* $C = (2\log(2))^{-1}$.

Given N, we denote by $\omega(N)$ the number of distinct prime factors of N. We fix a constant $\delta > 0$ for which Theorem 4.4 holds, and we denote by X the set of integers N that satisfy the inequalities

$$\begin{cases} \omega(N) \leq 2\log\log N, \\ \mathrm{ord}_B(N) = |H_N| \geq N^{\frac{1}{2}} \exp(\log(N)^\delta). \end{cases} \tag{8.5}$$

By Theorem 4.4 and the fact that the normal order of the function ω is $\log\log N$ (see [6, §22.1 and Theorem 431]), the set X is a set of full density.

Given $\varepsilon > 0$, let $r = r_{\varepsilon,\eta,k} > max(D_k, \Delta_B)$ be such that

$$\frac{1}{\zeta(2)} \sum_{n=1}^{r} \frac{1}{n^2} \geq 1 - \varepsilon. \tag{8.6}$$

Since the density of the set $\mathcal{F}$ of square-free integers is $\frac{1}{\zeta(2)}$ (see [6, Theorem 333]), and $\mathbf{N} = \sqcup_{n\geq 1} n^2\mathcal{F}$ (a disjoint union of sets of respective density $\frac{n^{-2}}{\zeta(2)}$), the set of integers for which the largest square factor is smaller than r^2 is of density at least $1-\varepsilon$.

We define Y_ε as the intersection of X with the set of integers bigger than e^{D_k}, whose largest square factors are smaller than r^2; the density of Y_ε is $\geq 1-\varepsilon$. We wish to show that every large enough integer $N \in Y_\varepsilon$ is contained in $X_{\eta,k}$.

Given $N \in Y_\varepsilon$, we can write $N = s_1^2 q_1$ where q_1 is square-free and $s_1 \leq r$. We will 'dump' the smallest prime factors of q_1 in the following way. Let I be the set of prime factors p of q_1 that satisfy

$$p \geq (\log N)^{\frac{8}{C\eta^2}}, \tag{8.7}$$

where C is the constant from Lemma 8.7; then, let J be the set of prime factors of q_1 strictly smaller than this bound. Set

$$q = \prod_{p \in I} p, \quad \text{and} \quad M = s_1^2 \prod_{p \in J} p. \tag{8.8}$$

Thus $N = Mq$, M and q are coprime, and since $N \geq e^{D_k}$, every $p \in I$ satisfies $p \geq D_k$ (indeed, $p \geq D_k^8$ since C and η are in $]0,1[$). Thus the chosen B, N, M, D_k, q, x_0, k satisfy the conditions (Ω).

We will need a bound on M, as follows. We have

$$M \leq r^2 \prod_{p \in J} p \leq r^2 (\log N)^{\frac{8}{C\eta^2}|J|}, \tag{8.9}$$

and from the bound $|J| \leq \omega(N) \leq 2 \log\log N$, we deduce

$$M \leq r^2 \exp\left(\frac{8}{C\eta^2}(\log\log N)^2\right). \tag{8.10}$$

By Theorem 7.12, we obtain

$$|\widehat{\mu_{x_0}}(k)|^4 \leq \sqrt{\frac{\omega}{\kappa}} + \frac{6^{\omega/2} M^{15} N}{|H_N|^2}, \tag{8.11}$$

where

$$\kappa = \inf_{p \in I} |H_p| \geq C \log(\log N)^{\frac{8}{C\eta^2}} = \frac{8}{\eta^2} \log\log N \tag{8.12}$$

by Lemma 8.7 and Equation (8.7), and

$$\omega \leq \omega(N) \leq 2 \log\log N. \tag{8.13}$$

Thus the first term $\sqrt{\omega/\kappa}$ is smaller than $\eta/2$. The second term satisfies

$$\frac{6^{\omega(N)/2} M^{15} N}{|H_N|^2} \leq \frac{\exp\left((\log 6)(\log\log N) + 30 \log r + \frac{120}{C\eta^2}(\log\log N)^2\right) N}{N \exp(2(\log N)^\delta)}, \tag{8.14}$$

by the bounds on $|H_N|$, $\omega(N)$ and M. Since $(\log\log N)^2 = o((\log N)^\delta)$, the above quantity is smaller than $\eta/2$ for N sufficiently large, let's say $N \geq N_{\eta,k,\varepsilon}$. Thus

$$Y_\varepsilon \cap [N_{\eta,k,\varepsilon}, +\infty) \subset X_{\eta,k},$$

so $X_{\eta,k}$ contains a subset of density $1 - \varepsilon$, where $\varepsilon > 0$ is arbitrary.

8.3.2. *Step 2.* We have shown that $X_{\eta,k}$ is a set of full density. The following observation is classical.

Lemma 8.8. *Let $(K_n)_{n\geq 1} \subset \mathbf{N}$ be a countable family of sets of full density. Then there exists a set $K \subset \mathbf{N}$ of full density such that for all n, $K \setminus K_n$ is finite.*

Proof. Changing K_n into the intersection of K_n with all K_m for $m \leq n$, we can assume that $K_{n+1} \subset K_n$ for all $n \geq 1$. Define K to be equal to K_n in the interval $[a_n, a_{n+1}]$, where $(a_n)_{n\geq 1}$ is an increasing sequence of integers to be chosen soon; then, $K \setminus K_n$ is finite because it is contained in $[0, a_{n+1}]$. Thus, we only need to choose the a_n in such a way that the density of K is 1. For this, we choose the a_n for $n \geq 1$ such that for all $x \geq a_n$, the density of K_n in $[a_1, x]$ is larger than $1 - 2^{-n}$. □

We apply the previous lemma to the countable family $(X_{1/n,k})$. This provides a set $K \subset \mathbf{N}$ of full density such that $\{N \in K : |\widehat{\mu_{x_0,N}}(k)|^4 > \eta\}$ is finite for any $k \neq 0$, $\eta > 0$; in other words, for any $k \neq 0$, the k-th Fourier coefficient tends to zero as N goes to infinity. By Weyl's criterion, $\mu_{x_0,N}$ equidistributes to the Haar measure when N tends to infinity in K, as required.

REFERENCES

[1] J. Bourgain and A. Glibichuk. Exponential sum estimates over a subgroup in an arbitrary finite field. *Journal d'Analyse Mathématique*, 115:51–70, 2011.

[2] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. The distribution of closed geodesics on the modular surface, and Duke's theorem. *Enseign. Math. (2)*, 58(3-4):249–313, 2012.

[3] Pál Erdös and M. Ram Murty. On the order of $a \pmod p$. In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 87–97. Amer. Math. Soc., Providence, RI, 1999.

[4] Kenneth Falconer. *Fractal geometry*. John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2003. Mathematical foundations and applications.

[5] Peter Freyd and Kevin S. Brown. Problems and Solutions: Solutions: E3410. *Amer. Math. Monthly*, 99(3):278–279, 1992.

[6] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[7] Pär Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.

[8] Pär Kurlberg and Zeév Rudnick. On quantum ergodicity for linear maps of the torus. *Comm. Math. Phys.*, 222(1):201–227, 2001.

[9] John Milnor. Introductory dynamics lectures, chapter 7. *Author webpage*, pages 1–22, 2022.

[10] Terence Tao and Van H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012].
[11] D. D. Wall. Fibonacci series modulo *m*. *Amer. Math. Monthly*, 67:525–532, 1960.
[12] Lai Sang Young. Dimension, entropy and Lyapunov exponents. *Ergodic Theory Dynam. Systems*, 2(1):109–124, 1982.

IRMAR (UMR 6625 DU CNRS), UNIVERSITÉ DE RENNES 1, FRANCE
Email address: serge.cantat@univ-rennes1.fr, francois.maucourant@univ-rennes1.fr